

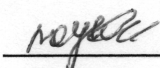
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему: «Дослідження використання методів та інструментів комп'ютерної
криміналістики при розслідуванні кіберінцидентів»

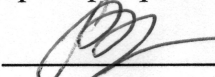
Виконав студент 4-го курсу групи КБ-19-2
спеціальності 125 «Кібербезпека»

 Андрій Опанасюк

Керівник доцент кафедри КІ та КБ, к.т.н., доцент

 Юрій Россінський

Рецензент професор кафедри КІ та КБ, д.т.н., доцент

 Володимир Воротніков

Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Опанасюк Андрій Миколайович

Тема роботи: «Дослідження використання методів та інструментів комп'ютерної криміналістики при розслідуванні кіберінцидентів»

затверджена Наказом університету від 1 березня 2023 р. № 99

Термін здачі студентом закінченої роботи 29 червня 2023 р.

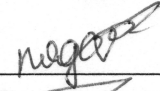
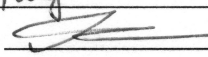
Вихідні дані роботи : Дослідження інструментів комп'ютерної криміналістики на базі ОС Windows.

Обладнання та програмне забезпечення:

1. ОС Windows
2. FTK imager
3. Volatility, Mimikatz
4. AutoSpy
5. Hack the browser data

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 01.03.2023	 01.03.2023
2	Єфіменко А.А.	 10.04.2023	 10.04.2023
3	Єфіменко А.А.	 20.04.2023	 20.04.2023

Студент  Опанасюк Андрій
Керівник  Юрій Россінський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2023-13.03.2023	
2	Ознайомлення з задачею	13.03.2023-29.03.2023	
3	Вивчення предметної області для виконання завдань	29.03.2023-15.04.2023	
4	Ознайомлення з принципами комп'ютерної криміналістики	16.04.2023-8.05.2023	
5	Ознайомлення з Інструментами	24.05.2023-03.06.2023	
6	Встановлення програмного забезпечення	04.06.2023-17.06.2023	
7	Налаштування та витяг даних	18.06.2023-20.06.2023	
8	Оформлення звіту	20.06.2023-26.06.2023	

Студент Андрій Опанасюк

Керівник Юрій Россінський

АНОТАЦІЯ

Кваліфікаційна роботи бакалавра викладена на 53 сторінках, вона містить 3 розділи, 38 рисунків, одну таблицю, 12 джерел в переліку посилань, розміщених на 2 сторінках.

Метою кваліфікаційної роботи є дослідження процесу розслідування кіберінцидентів і ознайомлення з інструментами комп'ютерної криміналістики для ефективного збору, аналізу та фіксації доказів у випадках кіберзлочинів.

Завдання, які будуть розглянуті в рамках цієї роботи, включають теорію комп'ютерної криміналістики, розглянення спеціального програмного забезпечення, аналіз різних джерел комп'ютерної інформації.

Ключові слова: ФОРЕНЗИКА, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, FTKIMAGER, VOLATILITY, MIMIKATZ, AUTOSPY, HACK DATA BROWSER.

					ККІК<.КР.Б – 125 – 12 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата		Лім.	Арк.	Аркушів
		Розроб.	Опанасюк А.М.	23.06.23	...Дослідження використання методів... та інструментів комп'ютерної кримі- налістики при розслідуванні кіберін- цидентів			
		Керівник	Росієвський Ю.М.	20.06.23				
		Реценз.	Воротніков В.В.	20.06.23				
		Н. контр.						
		Затверд.	Єфіменко А.А.	20.06.23		ФІКТ, Гр. КБ-19-2		

ANNOTATION

The bachelor's thesis is set out on 53 pages, it contains 3 chapters, 38 images, one table, 20 sources in the list of references, located on 2 pages.

The purpose of the qualification work is to study the process of investigating cyber incidents and to get acquainted with computer forensics tools for the effective collection, analysis and recording of evidence in cases of cybercrime.

The tasks that will be addressed in this paper include the theory of computer forensics, consideration of special software, analysis of various sources of computer information.

Keywords: FORENSICS, SOFTWARE, FTKIMAGER, VOLATILITY, MIMIKATZ, AUTOSPY, HACKDATA BROWSER.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієнський Ю.М				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ДОСЛІДЖЕННЯ ПРОЦЕСУ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ	9
1.1 Поняття цифрової криміналістики.....	9
1.2 Забезпечення цілостності доказового матеріалу	13
1.3 Збір та аналіз даних.....	14
1.4 Фіксація доказів та звіту	18
1.4 Постановка технічного завдання.....	19
РОЗДІЛ 2. ОГЛЯД ІНСТРУМЕНТІВ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ.....	20
2.1 Інструмент для створення образу ОС та дамів ОЗП.	20
2.2 Перехоплення даних користувача ОС Windows.	21
2.3 Автоматизоване ПЗ аналізу даних.....	23
2.4 Витягнення зашифрованих даних з браузерів.....	27
РОЗДІЛ 3 ПОСЛІДОВНЕ ДОСЛІДЖЕННЯ ОБРАЗУ ОС WINDOWS.....	29
3.1. Створення образу досліджуваної ОС.	29
3.2. Створення дампу ОЗП.....	31
3.3. Витягнення паролів користувачів.	33
3.4. Витягнення даних з дампу ОЗП.	37
3.5 Комплексний аналіз файлової системи за допомогою ПЗ Autospy	41
3.6 Витягнення даних браузера.....	50
ВИСНОВКИ.....	52
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	53
ДОДАТКИ.....	55

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

КТЕ – Комп'ютерна технічна експертиза

ОЗП – Оперативна пам'ять

Дамп – знімок інформації про стан комп'ютерної системи

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В сучасному світі технології розвиваються швидко, дані активно цифриізуються. Разом з цим збільшується кількість кіберзлочинів та інцидентів в сфері інформаційних технологій. З кожним роком збільшуються способи шахрайства різних інформаційних системах.

Для заподії та розкритів кіберзлочинів фахівці з комп'ютерної криміналістики розробляють нові можливості аналізу та реагування проти сучасних кіберзлочинців. Технічний прогрес дає можливість скоювати злочини новими способами і за допомогою нових знарядь. Тією ж мірою прогрес сприяє появі нових способів розкриття злочинів - як старих, так і нових.

Метою кваліфікаційної роботи є дослідження та застосування основного програмного забезпечення для аналізу та розслідування кіберінцидентів.

Визначена мета обумовлює наступні завдання:

- Дослідження прийомів та способів збору цифрових даних
- Забезпечення цілісності доказового матеріалу
- Застосування методів та інструментів для ефективного збору цифрових даних
- Оцінка результатів

Об'єктом дослідження є процесотримання доказів засобами цифрової криміналістики.

Предметом дослідження є збір основної цифрової інформації, доказів з персонального комп'ютера. На базі ОС Windows та інструментів форензіки.

У процесі виконання кваліфікаційної роботи було розроблено проект спрямований на розробку та впровадження комп'ютерної криміналістики для ефективного знаходження доказів, включаючи забезпечення цілісності матеріалу, збір та аналіз даних, фіксацію.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієський Ю.М				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ДОСЛІДЖЕННЯ ПРОЦЕСУ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

1.1 Поняття цифрової криміналістики

Форензика - наука, що вивчає методи і техніки збирання, аналізу та інтерпретації фізичних та цифрових доказів злочинів та встановлення подій у судових справах. Форензичні науковці використовують свої навички, щоб допомогти правоохоронним органам, суду і приватним компаніям розкрити кіберінциденти та кіберзлочини.

Термін “форензика” походить від латинського “foren”, що означає “промова перед форумом”, тобто виступ перед судом, судові дебати - це був один з улюблених жанрів у Стародавньому Римі.

До 1970-х років розгляд злочинів з використанням комп'ютерів проводився на підставі чинних законів. Уперше, як самостійний вид злочинів, комп'ютерні злочини були закріплені в 1978 році в Законі штату Флориди про комп'ютерні злочини, що містив законодавство проти несанкціонованої зміни або видалення даних у комп'ютерній системі. Упродовж наступних років кількість видів злочинів, скоєних із використанням комп'ютерів, зростала, що призвело до ухвалення законів, що регулювали сфери авторського права, приватності.

Тільки з 80-х років злочини з використанням комп'ютерів стали включати до федеральних законів. Першою країною, яка ухвалила такий закон у 1983 р., стала Канада. Потім послідував Федеральний закон США - "Закон про комп'ютерне шахрайство і зловживання".

Зростання комп'ютерної злочинності у 80-х і 90-х роках ХХ століття спричинило необхідність створення правоохоронними органами окремих держав груп спеціального призначення для вирішення технічних аспектів розслідувань комп'ютерних злочинів. Приміром, у США, у 1984 р. ФБР запустив "Команду комп'ютерного аналізу та реагування", а наступного року в столичній поліції Великої Британії був створений і почав свою роботу відділ проти шахрайства. Крім того, що вони були професіоналами в правоохоронних органах, багато хто з перших членів цих груп були також любителями комп'ютерів і стали відповідальними за початкові дослідження і напрямки у цій галузі.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		9

З 2000 року виникає потреба в стандартизації, різні органи й агентства починають публікувати документи, що встановлюють керівні принципи цифрової криміналістики. Наукова робоча група з цифрових свідчень підготувала доповідь 2002 року на тему "Найкращі практики комп'ютерної криміналістики", за цим послідувала публікація в ISO стандарту.

Набула чинності Конвенція про кіберзлочинність у 2004р. Метою підписантів цього документа було узгодження своїх національних законів про комп'ютерні злочини, методів розслідування та міжнародного співробітництва.

У 2009 році була опублікована доповідь Петерсона і Шеноя під назвою "Цифрові криміналістичні дослідження: хороше, погане і безрезультатне", в якій вони відзначили присутність упередженості серед деяких експертів-криміналістів щодо операційної системи Windows під час проведення цифрових криміналістичних досліджень.

Симсон Гарфінкель висунула проблеми, з якими цифрові розслідування можуть зіткнутися у майбутньому. Вона вказала на зростаючий обсяг цифрових носіїв, загальну доступність шифрування для користувачів, різноманітність операційних систем і форматів файлів, збільшення кількості осіб, які мають кілька пристроїв, а також наявні юридичні обмеження для слідчих.

Ці дві роботи свідчать про те, що у комп'ютерної форензики виникають нові виклики та проблеми, пов'язані з технологічними та правовими аспектами. Це вимагає оновлення інструментів, а також удосконалення фахівців.

Сфери застосування форензики:

1. Розкриття та розслідування кримінальних злочинів, у яких фігурує комп'ютерна інформація як об'єкт посягання, комп'ютер як знаряддя вчинення злочину, а також будь-які цифрові докази.

2. Збирання та дослідження доказів для цивільних справ, коли такі докази мають вигляд комп'ютерної інформації. Докази мають вигляд комп'ютерної інформації. Особливо це актуально при порушенні прав інтелектуальної власності.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		10

3. Страхові розслідування, що проводяться страховими компаніями щодо можливих порушень умов договору, страхового шахрайства, особливо коли об'єкт страхування представлений у вигляді комп'ютерної інформації.

4. Внутрішньокорпоративні розслідування інцидентів безпеки, що стосуються інформаційних систем, а також роботи із запобігання витоку інформації, що містить ацценію витоку інформації, що містить комерційну таємницю.

5. Військові та розвідувальні завдання з пошуку, знищення та відновлення комп'ютерної інформації під час чинення впливу на інформаційні системи противника та захисту своїх систем.

6. Завдання щодо захисту громадянами своєї особистої інформації в електронному вигляді, самозахисту своїх прав. Це пов'язано з електронними документами та інформаційними системами.

Комп'ютерно-технічної експертиза є самостійним родом судових експертиз. Вона належить до класу інженерно-технічних експертиз. КТЕ проводять з метою визначення статусу об'єкта як комп'ютерного засобу, виявлення та вивчення його слідової картини в розслідуваному злочині, отримання доступу до інформації на носіях даних. КТЕ поділяється на декілька видів:

1. Цифрове розслідування - процес виявлення та розслідування кіберзлочинів. Він включає в себе аналіз цифрових слідів, таких як логи систем, електронна пошта, файли журналів та інші електронні докази. Цифрові розслідування можуть допомогти ідентифікувати злочинця, встановити зв'язки між різними доказами та відновити хронологію подій.

2. Відновлення видалених даних - експерти використовують спеціальні методи та інструменти для відновлення видалених або втрачених даних з комп'ютерних систем та зберігаючих пристроїв. Це може бути корисним в розслідуванні, оскільки відновлені дані можуть містити важливу інформацію про злочин і злочинця.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росііський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		11

3. Аналіз мережі - вивчається мережевий трафік і аналізують його для виявлення незаконних дій, вторгнень у систему, крадіжок даних або зловживань привілеями. Вони можуть ідентифікувати підозрілі активності, шляхи атак та слабкі місця в мережі.

4. Експертиза цифрових доказів включає аналіз інформації, знайденої на комп'ютерних системах, мобільних пристроях або інших електронних пристроях. Вони визначають достовірність доказів, перевіряють їх цілісність для судового процесу.

Важливість послідовності в комп'ютерній форензиці - кроки для успішного розслідування.

Послідовність дій в комп'ютерній форензиці

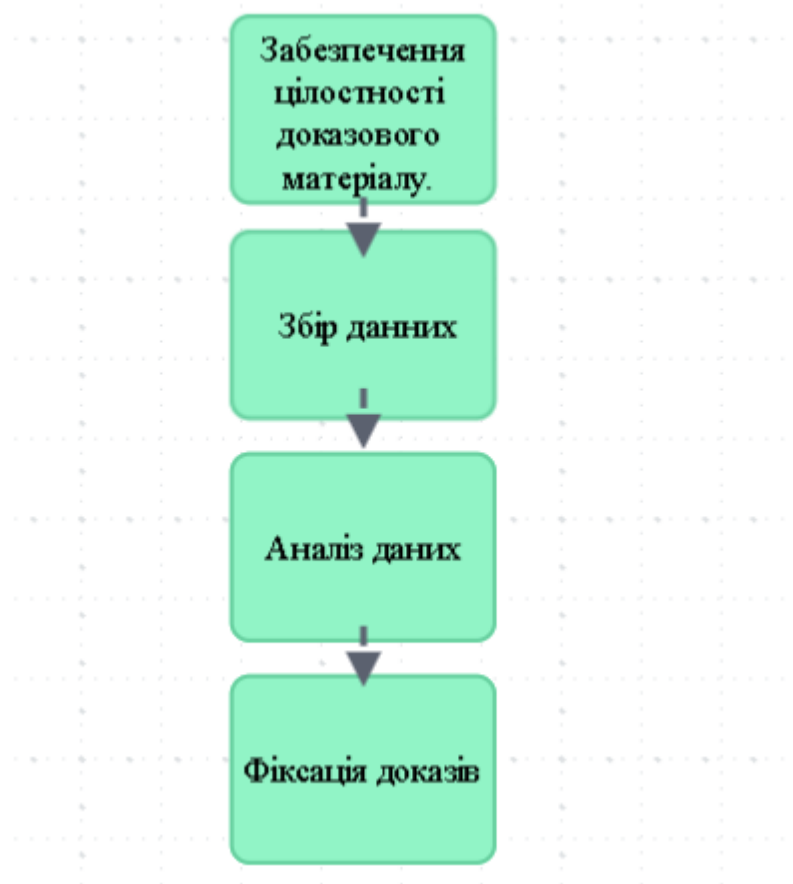


Рисунок 1 – Послідовність дій

1.2 Забезпечення цілостності доказового матеріалу

Головним пріоритетом під час розслідування кіберінцидентів є збереження цілісності зібраних доказів. Забезпечення того, щоб докази залишалися незмінними, гарантує об'єктивність і достовірність для цілей свідчень.

Вкрай важливо розглянути можливість впровадження фізичних заходів безпеки для таких речових доказів. Криптографічні методи зазвичай використовуються для підтримки цілісності даних. Щоб запобігти несанкціонованому доступу або змінам, можна застосувати шифрування. Крім того, впровадження хеш-функцій дає змогу перевірити цілісність доказів шляхом порівняння вихідних і повторюваних хеш-значень.

Важливо документувати всі етапи обробки доказів; таким чином вимагається ведення журналів реєстрації, реєстрація позначок часу, обмеження доступу до доказового матеріалу.

Збереження цілісності доказового матеріалу в процесі розслідування має важливе значення для забезпечення об'єктивних і достовірних доказів для судових і правоохоронних проваджень. Для ефективного досягнення цієї мети необхідно використовувати спеціалізоване програмне забезпечення, здатне точно створювати побітові копії.

Майже всі сліди, з якими доводиться працювати фахівцеві з форензики, мають вигляд комп'ютерної інформації. Їх досить легко знищити - як навмисне, так і випадково. Часто їх легко підробити, бо "підроблений" байт нічим не відрізняється від "справжнього". Цифрові докази можнатільки за посередництвом складних апаратнопрограмних засобів. Тому ці сліди складно продемонструвати іншим особам - понятим, прокурору, судді. Не завжди просто забезпечити незмінність слідів при їх зберіганні. І не тільки забезпечити, а й довести суду цю незмінність. Поняття "незмінність" лише з натяжкою можна застосувати до комп'ютерної інформації.

На деяких видах носіїв вона зберігається дійсно статично - у вигляді різної намагніченості ділянок носія або варіацій його оптичних властивостей носія.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Россінський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		13

Оперативна пам'ять комп'ютера (типу DRAM) регенерується раз на кілька мілісекунд. Тобто записані там сигнали фактично стираються і записуються знову.

1.3 Збір та аналіз даних

Важливий етапом в процесі комп'ютерної форензики, оскільки саме на цьому етапі збираються цифрові докази, які далі аналізуються та використовуються у розслідуванні кримінальних справ. Збір здійснюється з різних джерел, таких як комп'ютери, мобільні пристрої, цифрові носії, мережі і інші електронні пристрої.

Захоплення образів дисків найпоширеніший з методів збору даних в комп'ютерній форензиці. Це означає створення точної копії цифрового носія, такого як жорсткий диск або USB-накопичувач, з метою збереження всієї інформації, включаючи видалені файли, метадані і структуру файлової системи.

Основна мета захоплення образу полягає в тому, щоб забезпечити цілісність і незмінність даних, запобігти їх втраті або пошкодженню під час процесу розслідування. Фахівець повинен ретельно спланувати процес захоплення образу. Це включає визначення цілей розслідування, вибір методів захоплення та вибір відповідного обладнання та програмного забезпечення для проведення процесу.

Існує кілька методів захоплення образу, які можуть бути використані в залежності від характеристик об'єкта, що вивчається, та цілей розслідування. Деякі з поширених методів включають фізичне копіювання диска, логічне копіювання файлів, захоплення пам'яті та захоплення мережевого трафіку.

Спеціаліст повинен підготувати необхідне обладнання для збору образу. Це може включати в себе переносний комп'ютер або розширювальний пристрій, зовнішні накопичувачі даних, програмне забезпечення для захоплення образу, кабелі та інші аксесуари.

Далі розпочинається процес захоплення образу. Застосовуючи вибраний метод, фахівець копіює цифрові дані з об'єкта, що вивчається, забезпечуючи їх цілісність та незмінність. Важливо виконувати цей крок у контрольованому середовищі, щоб уникнути потенційних пошкоджень або змін у даних.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Після завершення захоплення образу необхідно перевірити його цілісність і надійність. Це включає порівняння хеш-сум або контрольних сум файлів образу з оригінальними даними для підтвердження їх ідентичності. Крім того, важливо докладно задокументувати процес захоплення образу, включаючи дату, час, використання обладнання та програмне забезпечення, що допомагають забезпечити цілісність доказів.

Образ необхідно зберегти у безпечному місці. Це може бути захищений сервер або зовнішній носій даних, що забезпечує надійну збереження і захист образу від втрати або пошкодження.

Витягування даних зі смартфонів і мобільних пристроїв збір даних з цих пристроїв став дедалі важливішим. Фахівці з форензики використовують спеціальні програми та методики для отримання доступу до даних на смартфонах, таких як повідомлення, контакти, фотографії, вихідні дані з додатків тощо.

Мережевий моніторинг пов'язаний з мережевою активністю, використовуються методи мережевого моніторингу. Це включає реєстрацію мережевого трафіку, аналіз журналів серверів, перехоплення пакетів із використанням спеціальних інструментів для виявлення підозрілих або зловмисних дій. Для аналізу інтернет-активності користувача необхідно визначити встановлені браузері і провести для них аналіз артефактів:

- файли історії відвідування (index.dat, sqlite тощо);
- тимчасові директорії;
- куки (cookies);
- кеш сторінок;
- обране, закладки;
- панелі інструментів;
- плагіни;

Відновлення видалених даних: Іноді важливі дані можуть бути випадково видалені або намагатися приховати. Фахівці з комп'ютерної форензики використовують спеціальні програми та методи для відновлення видалених файлів або діапазонів даних з цифрових носіїв, таких як жорсткі диски, флеш-пам'ять тощо.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Коли користувач видаляє файл з комп'ютера, він фактично не зникає повністю з носія даних. Застосування методів, таких як копіювання секторів диска або відновлення файлових систем, дозволяє відновити видалені файли. Це може бути корисно для отримання доступу до важливих доказів, які можуть бути приховані.

Фахівець використовує спеціальні програми або скрипти, що аналізують структуру диска та відновлюють файли на основі їх сигнатур або характеристик. Цей метод дозволяє відновити видалені файли, навіть якщо їх заголовки або файлові системи були пошкоджені.

Неалокаційний простір є частиною диска, яка не використовується для зберігання файлів або інформації про них. Його аналіз може містити сліди видалених файлів, фрагменти тексту, зображень або інші важливі дані.

У випадку, коли дані були зашифровані або захищені паролем, фахівці з форензики можуть застосовувати методи відновлення паролів або криптоаналізу для отримання доступу до зашифрованої інформації. Це може включати використання словникових атак, перебору паролів або використання спеціальних інструментів для взлому шифрування.

Аналіз реєстраційних записів і журналів, вони зберігаються в операційних системах та програмах, можуть містити важливу інформацію про дії користувачів, події, виконані команди та інші подробиці. Аналіз допоможе виявити активності пов'язані зі злочином.

Слідчий або оперуповноважений спільно з фахівцем

і понятими проводить огляд вмісту комп'ютера. При цьому використовуються штатні програмні та апаратні засоби. Складається протокол огляду, де відображається:

- характеристики сервера, версія ОС;
- наявність і робочий стан програми, що генерує логи;
- наявність файлів із логами, їхні часові мітки;
- права доступу до логфайлів;
- облікові записи користувачів, які мають права на запис у логфайли.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Россінський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Потрібні записи з потрібних логів вибираються за допомогою відповідних фільтрів, роздруковуються на принтері та додаються до протоколу огляду.

Усі аркуші протоколу і додатків підписують учасники огляду.

Аналіз даних - ключовий етап у комп'ютерній форензиці, який Цей процес дозволяє фахівцям з форензики з'ясувати подробиці кримінальних подій, встановити зв'язки між даними та отримати важливі відомості для розслідування.

Основна мета аналізу використанням спеціалізованого ПЗ полягає в отриманні доказів, які можуть бути використані в судовому процесі для встановлення фактів та підтвердження злочинної діяльності.

Проводиться детальний перегляд файлів і директорій на цифрових пристроях. Експерти вивчають назви файлів, розташування, розширення та вміст, щоб визначити наявність потенційно важливих доказів. До файлів можуть входити текстові документи, електронна пошта, зображення, відео, аудіофайли, бази даних тощо.

Переглядаються журнали та лог-файли, які містять інформацію про активність користувачів, події системи, мережеву активність тощо. Це може допомогти виявити злочинну діяльність.

Фахівець з форензики використовує спеціальні методи та інструменти для виявлення прихованої інформації у файловій системі. Це можуть бути зашифровані файли, стеганографічні повідомлення, приховані розділи диску, змінені атрибути файлів.

Аналіз оперативної пам'яті (ОЗП) в комп'ютерній форензиці є важливим етапом розслідування, вона зберігає тимчасову інформацію, яка може бути важливою для виявлення злочинної діяльності, ідентифікації злочинців або відновлення подій.

Отриманий образ ОЗП піддається детальному аналізу. Досліджується вміст пам'яті, що включає в себе запущені процеси, відкриті файли, пам'яткові структури, реєстри, іншу інформацію. Це дозволяє отримати уявлення про активність користувача.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Фахівець аналізує структуру даних в ОЗП для виявлення аномалій або несподіваних паттернів, які можуть свідчити про злочинну діяльність. Це включає перевірку вмісту реєстрів, таблиць процесів, схеми пам'яті та інші елементи, які можуть містити важливу інформацію.

Аналіз ОЗП є потужним інструментом у комп'ютерній форензиці, оскільки він дозволяє отримати цінні докази, які можуть розкрити злочинну діяльність, ідентифікувати злочинців або відновити події. Навіть пароль не надається можна зробити дамп ОЗП та спробувати відновити паролі до вимикнення системи.

1.4 Фіксація доказів та звіту

Фіксація доказів та складання звіту є важливими етапами в роботі фахівців з форензики. Ці процеси забезпечують коректність та достовірність зібраних даних і дозволяють зберегти їх для подальшого використання в судових процедурах.

Кожен зібраний доказ повинен бути детально задокументований. Це включає опис доказу, дату і час його збору, місце, з якого він був отриманий, і будь-яку іншу важливу інформацію. Документація також може включати фотографії, відео або інші матеріали, які підтверджують стан доказу на момент його збору.

На основі аналізу доказів фахівець з форензики встановлює факти, які можуть мати вирішальне значення для розслідування. Це може включати ідентифікацію осіб, встановлення часових рамок подій, розкриття злочинів, виявлення зловживань тощо. Звіт повинен бути чітким, об'єктивним і логічно структурованим, щоб інші фахівці або сторони розуміли представлену інформацію.

Фахівець може бути запрошений як свідок у судовому процесі, де він представляє свідчення доказів та результатів аналізу. Він повинен бути готовим до відповідей на запитання сторін, що ведуть справу, а також до пояснення технічних аспектів своєї роботи.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		18

1.4 Постановка технічного завдання

Провести загальне дослідження інструментів комп'ютерної криміналістики.

Інструменти для створення образу операційної системи та дамів оперативної пам'яті дозволяє створювати точні копії для подальшого аналізу.

Перехоплення даних користувача операційної системи Windows. Огляд інструментів, що дозволяють отримувати доступ до паролів, ключів шифрування та інших конфіденційних даних, які зберігаються у пам'яті комп'ютера.

Дослідити автоматизоване програмне забезпечення для аналізу даних. Воно надає можливість виконувати комплексний аналіз файлової системи, виявляти зображення, аналізувати комунікації, події Windows та витягувати інші важливі дані.

Головною частиною технічного завдання є послідовне дослідження образу ОС Windows. Ця частина має такий план:

1. Створення копій за допомогою ПЗ FTK imager.
2. Створення образу досліджуваної ОС.
3. Створення дампу оперативної пам'яті.
4. Витягнення даних з дампу ОЗП
5. Комплексний аналіз файлової системи за допомогою ПЗ Autopsy.
 - 5.1. Виявлення та аналіз зображень.
 - 5.2. Аналіз модулів.
 - 5.3. Аналіз подій Windows.
 - 5.4. Додаткові функції.
6. Витягнення даних браузера з використанням спеціального ПЗ.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		19

РОЗДІЛ 2. ОГЛЯД ІНСТРУМЕНТІВ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ.

2.1 Інструмент для створення образу ОС та дамів ОЗП.

Криміналістичний образ найчастіше потрібен для перевірки цілісності образу після вилучення жорсткого диска. Зазвичай це роблять правоохоронні органи для суду, оскільки після створення образу можна перевірити його цілісність, щоб переконатися, що він не був підроблений.

Основна функція FTK Imager полягає в створенні образу диска або пристрою для подальшого аналізу. Образ диска - це точна копія всієї інформації, що зберігається на дисках або пристрої, включаючи вміст файлів, відомості про систему та інші метадані. Образ диска може бути використаний для аналізу даних, пошуку доказів або відновлення втрачених файлів.

FTK Imager підтримує кілька форматів збереження образів диска, включаючи EnCase, SMART та RAW. Інструмент також може працювати зі збереженими образами диска, дозволяючи проводити різноманітний аналіз даних, включаючи пошук тексту, перегляд файлів та відновлення втрачених файлів. FTK Imager є потужним інструментом для збору доказів та аналізу електронних даних. Інструмент підтримує безліч форматів файлів і дисків, що дозволяє проводити дослідження в широкому діапазоні областей.

Ви також можете переглянути вміст зображень, які можуть зберігатися на локальному комп'ютері або диску.

Можна змонтувати образ для переглядів в режимі "тільки для читання", що також дозволить вам переглянути вміст образу в тому вигляді, в якому користувач бачив його на оригінальному носії.

Переглядати і відновлювати файли, які були видалені з Кошика, але ще не були перезаписані на дисках.

Захоплення дампу - це метод захоплення і скидання вмісту енергозалежної пам'яті на енергонезалежний накопичувач, щоб зберегти його для подальшого дослідження. Аналіз флеш-накопичувача може бути успішно проведений тільки тоді, коли зчитування було виконано точно, без пошкодження образу енергонезалежної пам'яті. На цьому етапі слідчий повинен бути обережним у своїх рішеннях щодо

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росініський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		20

збору енергозалежних даних, оскільки після перезавантаження системи вони не існуватимуть.

2.2 Перехоплення даних користувача ОС Windows.

Перехоплення даних користувача ОС Windows є важливою складовою комп'ютерної криміналістики під час розслідування кіберінцидентів. Два популярних інструменти, що використовуються для цього - Mimikatz та Volatility.

Mimikatz - це застосунок із відкритим вихідним кодом, який дає змогу користувачам переглядати та зберігати облікові дані аутентифікації, як-от тікети Kerberos.

Зловмисники зазвичай використовують Mimikatz для крадіжки облікових даних і підвищення привілеїв: у більшості випадків програмне забезпечення для захисту кінцевих точок і антивірусні системи виявляють і видаляють його. І навпаки, фахівці з тестування на проникнення використовують Mimikatz для виявлення і тестування вразливостей у ваших мережах, щоб ви могли їх виправити.

Спочатку Mimikatz демонстрував, як використовувати одну вразливість у системі аутентифікації Windows. Тепер же цей інструмент охоплює кілька різних видів вразливостей. Mimikatz може виконувати такі методи збору облікових даних:

Pass-the-Hash (перехоплення хеша): раніше Windows зберігав дані аутентифікації в хеші NTLM. Зловмисники використовують Mimikatz для передавання точного рядка хеша на цільовий комп'ютер задля в систему. Зловмисникам навіть не потрібно зламувати пароль, їм просто потрібно перехопити хеш і використовувати його без будь-якої обробки. Це те саме, що знайти ключ від усіх дверей будинку на підлозі. Вам потрібен один ключ, щоб відкрити будь-які двері.

Pass-the-Ticket (перехоплення тикета): нові версії Windows зберігають дані аутентифікації в конструкції, яка називається тикетом (Ticket). Mimikatz надає користувачеві можливість передати тикет Kerberos на інший комп'ютер і увійти в систему за допомогою цього тикета. В іншому це те ж саме, що і перехоплення і передача хеша.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Россинський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Over-Pass the Hash (Pass the Key): ще один різновид атаки pass-the-hash, але цей метод передає унікальний ключ для видачі себе за користувача, дані якого можна отримати від контролера домену.

Kerberos Golden Ticket): це різновид атаки з перехопленням тикета (pass-the-ticket), але в цьому разі метою є конкретний тикет для прихованого облікового запису під назвою KRBTGT. Цей обліковий запис шифрує всі інші тикети. "Золотий квиток" дає вам облікові дані адміністратора домену для будь-якого комп'ютера в мережі без терміну закінчення.

Kerberos Silver Ticket: ще одна атака типу pass-the-ticket, але "срібний тикет" використовує для своїх цілей функцію Windows, яка спрощує використання служб у мережі. Kerberos надає користувачеві тикет сервера видачі дозволів, і користувач може використовувати цей тикет задля входу у будь-які служби в мережі. Microsoft не завжди перевіряє тикет сервера видачі дозволів після його випуску, тому з його допомогою можна легко обійти будь-які заходи безпеки.

Volatility Forensics - аналіз оперативної пам'яті комп'ютера, є важливим інструментом у сфері цифрового форензіку. Цей метод дозволяє експертам отримувати цінну інформацію, яка може бути втрачена або прихована в інших джерелах дослідження, таких як жорсткий диск або журнали подій.

Волатильність оперативної пам'яті комп'ютера означає, що дані зберігаються лише на протязі роботи комп'ютера і втрачаються при вимкненні живлення. Проте, протягом роботи, важлива інформація може зберігатися у вигляді процесів, потоків, реєстраційних записів, паролів, криптографічних ключів та інших даних, що мають значення для проведення розслідування.

Для аналізу волатильності оперативної пам'яті використовуються різноманітні інструменти та методи. Один з них - Volatility Framework, який є потужним інструментом з відкритим кодом для аналізу пам'яті. Він надає можливість експертам проводити різноманітні операції, такі як відновлення процесів, аналіз структури даних, пошук підозрілих об'єктів та витягування важливої інформації.

Застосування Volatility Forensics може бути широким. Він допомагає у розслідуванні кібератак, крадіжки даних, шпигунства та інших злочинів, пов'язаних з

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		22

комп'ютерною безпекою. Експерти з волатильності можуть виявити активні процеси, виконувані команди, підозрілі зміни у системі, ключі шифрування та інші важливі деталі, що допомагають встановити причини та виявити злочинців.

Проте, аналіз волатильності оперативної пам'яті також має свої виклики. Пам'ять може бути зашифрована або захищена від доступу, а деякі шкідливі програми можуть намагатися знищити або приховати свої сліди у пам'яті. Тому експертам потрібно мати глибокі знання про комп'ютерну архітектуру, операційні системи та методи аналізу, щоб успішно проводити Volatility Forensics.

Завдяки розвитку цифрових технологій і зростанню кількості кіберзлочинності, Volatility Forensics стає все більш важливим інструментом для виявлення, розслідування та протидії кіберзлочинності. Експерти з волатильності оперативної пам'яті вносять вагомий внесок у сфери форензики, забезпечуючи належне розслідування кіберінцидентів і забезпечуючи безпеку цифрового світу.

2.3 Автоматизоване ПЗ аналізу даних

У світі цифрової криміналістики і форензіки, швидкість та точність виявлення інформації є ключовими факторами для успішного розслідування злочинів. Одним з найпотужніших інструментів, що застосовуються у цих областях, є Autospy - автоматизоване програмне забезпечення для аналізу даних.

Autospy є відкритим та безкоштовним програмним забезпеченням, розробленим спеціально для цифрової форензіки. Воно надає цифровим експертам доступ до широкого спектру інструментів і можливостей для збору, аналізу та інтерпретації цифрових доказів.

Autospy може бути використано для обробки різних видів даних, включаючи комп'ютерні файли, журнали подій, системну інформацію, аудіо- та відеозаписи, зображення, архіви та багато іншого. Воно дозволяє цифровим експертам отримати доступ до цих даних та проводити ретельний аналіз для виявлення слідів злочину, ідентифікації злочинців та відновлення подій, що сталися. Однією з найважливіших особливостей Autospy є його здатність автоматизувати багато процесів, пов'язаних з аналізом даних. Воно може швидко і ефективно обробляти

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		23

великі обсяги даних та виконувати автоматичний пошук ключових слів, створення звітів, генерацію графічних представлень даних та багато іншого. Це значно прискорює процес аналізу і дозволяє цифровим експертам зосередитися на більш складних завданнях, в той час як рутинні процеси виконуються автоматично.

Autopsy також має потужну систему фільтрації та пошуку, що дозволяє знаходити цінні дані та зв'язки між ними. Воно підтримує різні методи аналізу, включаючи кластеризацію, асоціативні правила, таймлайни, графи і багато іншого. Це допомагає експертам відновлювати послідовність подій, розуміти залежності та знаходити ключові докази.

Завдяки своїм потужним функціям і великому спектру можливостей, Autopsy став незамінним інструментом для цифрових експертів у сфері форензики. Він допомагає збирати надійні докази, встановлювати факти та допомагає правоохоронним органам виявляти та переслідувати кримінальні діяння.

Autopsy - це графічний інтерфейс до інструментів цифрового аналізу командного рядка в The Sleuth Kit. Разом вони можуть аналізувати диски і файлові системи Windows і UNIX.

Autopsy мають відкритий вихідний код і працюють на платформах UNIX/Оскільки Autopsy базується на HTML, ви можете підключитися до сервера Autopsy з будь-якої платформи за допомогою HTML-браузера. Autopsy має інтерфейс, подібний до "Файлового менеджера", і показує детальну інформацію про видалені дані та структури файлової системи.

Режими аналізу:

Мертвий аналіз: відбувається, коли для дослідження даних з підозрілої системи використовується спеціальна система аналізу. У цьому випадку Autopsy запускаються в довіреному середовищі, як правило, в лабораторії. Autopsy і TSK підтримують формати файлів raw, Expert Witness і AFF.

Аналіз у реальному часі: підозрювана система аналізується під час її роботи. У цьому випадку Autopsy запускаються з компакт-диска в ненадійному середовищі. Це часто використовується під час реагування на інцидент, поки інцидент

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росініський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		24

підтверджується. Після того, як інцидент підтверджено, систему можна отримати і провести аналіз "мертвого" комп'ютера.

Методи пошуку доказів:

Список файлів: Аналіз файлів і каталогів, включаючи імена видалених файлів і файлів з іменами в кодуванні Unicode.

Вміст файлів: Вміст файлів можна переглядати в сирому вигляді, в шістнадцятковому форматі або витягувати рядки ASCII. Коли дані інтерпретуються, Autopsy очищає їх, щоб запобігти пошкодженню локальної системи аналізу.

Autopsy не використовує жодних мов сценаріїв на стороні клієнта.

Хеш-бази даних: Пошук невідомих файлів у хеш-базі даних, щоб швидко визначити, чи є вони хорошими чи поганими. Autopsy використовує Національну довідкову бібліотеку програмного забезпечення NIST і створені користувачем бази даних відомих хороших і відомих поганих файлів.

Сортування за типом файлів: сортувати файли на основі їхніх внутрішніх сигнатур, щоб ідентифікувати файли відомого типу. Розтин також може витягувати лише графічні зображення. Розширення файлу також буде порівняно з типом файлу, щоб виявити файли, розширення яких, можливо, було змінено з метою їх приховування.

Часова шкала активності файлу: у деяких випадках наявність часової шкали активності файлів може допомогти виявити області файлової системи, які можуть містити докази. Autopsy може створювати часові шкали, які містять записи про час модифікації, доступу та зміни (MAC) як розподілених, так і нерозподілених файлів.

Пошук за ключовими словами: пошук за ключовими словами в образі файлової системи можна виконувати за допомогою ASCII-рядків і регулярних виразів *grep*. Пошук можна виконувати як у повному образі файлової системи, так і у нерозподіленому просторі. Для прискорення пошуку можна створити індексний файл. Рядки, які часто шукаються, можна легко налаштувати в Autopsy для автоматичного пошуку.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росініський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Аналіз метаданих: Структури метаданих містять детальну інформацію про файли і каталоги. Autopsy дозволяє переглянути деталі будь-якої структури метаданих у файловій системі. Це корисно для відновлення видаленого вмісту. Autopsy виконає пошук в каталогах, щоб визначити повний шлях файлу, який виділив структуру.

Аналіз блоків даних: Блоки даних - це місця, де зберігається вміст файлу. Autopsy дозволяє переглядати вміст будь-якого блоку даних у різних форматах, зокрема ASCII, hexdump і рядки. Також можна вказати тип файлу, і Autopsy виконає пошук у мета-структурах даних, щоб визначити, яка з них виділила блок даних.

Деталі зображення: Можна переглянути відомості про файлову систему, зокрема розміщення файлів на дисці і час їхньої активності. Цей режим надає інформацію, яка може бути корисною під час відновлення даних.

Керування справами

Керування справами: Розслідування організовано за кейсами, які можуть містити один або кілька хостів. Кожен хост налаштовується на власний часовий пояс і зміщення годинника так, щоб час, показаний на ньому, відповідав тому, який бачив би користувач, який його створив. Кожен хост може містити один або декілька образів файлової системи для аналізу.

За замовчуванням Autopsy генерує значення MD5 для всіх файлів, які імпортуються або створюються. Цілісність будь-якого файлу, який використовує Autopsy, можна перевірити у будь-який час.

Звіти: Autopsy може створювати звіти у форматі ASCII для файлів та інших структур файлової системи. Це дозволяє швидко створювати узгоджені таблиці даних під час дослідження.

Особливу увагу треба приділити увагу модулям ПЗ AutoSpry. Модулі це інструменти, які виконують аналіз нашої системи. Кожен має свій функціонал:

1)Recent Activity - це модуль вивчення недавніх дій користувача. Він витягує дані операційної системи, а також інформацію про останні дії користувача.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		26

2)Hash Lookup - якщо цей модуль увімкнено, то Autopsy обчислюватиме хеш-суму для знайдених файлів і порівнюватиме її зі значенням у базі даних.

3)File Type Identification - цей модуль ідентифікує тип файлу. Причому він зрозуміє, який це файл, навіть якщо у нього відсутнє або змінено розширення.

4)Extension Mismatch Detector - цей модуль шукає файли, у яких розширення не відповідає типу файлу.

5)Picture Analyzer - цей модуль аналізує зображення і витягує метадані.

6)Keyword Search - модуль пошуку за ключовими словами витягує потрібний нам текст зі знайдених файлів. Для його роботи потрібні словники. У комплекті вже є словники, налаштовані на пошук телефонних номерів, IP-адрес, адрес електронної пошти, посилань і номерів банківських карт.

7)Email Parser - цей модуль ідентифікує файли електронних повідомлень, а також витягує з них вкладені файли, додаючи їх у звіт.

8)Encryption Detection - шукає зашифровані файли або томи. Наприклад може знаходити розділи BitLocker, томи VeraCrypt.

9)PhotoRec Carver - якщо на джерелі даних є не розподілений простір, цей модуль спробує знайти файли, які раніше там були, і спробує їх відновити.

10)Virtual Machine Extractor - шукає файли віртуальних машин

11)Plaso - запускає інструмент Plaso. Аналізує купу всього, щоб витягти тимчасові мітки та побудувати таймлайн усіх подій у системі

2.4 Витягнення зашифрованих даних з браузерів

У сучасному цифровому світі, браузери стали важливими інструментами для нашої щоденної діяльності в Інтернеті. Ми використовуємо для перегляду веб-сторінок, здійснення покупок, входу в соціальні мережі та багато іншого. Однак, ці браузери також зберігають велику кількість наших особистих даних, які можуть бути зашифровані для забезпечення конфіденційності.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Витягнення зашифрованих даних з браузерів стало важливим завданням для цифрових форензичних експертів та кібербезпекових фахівців. Це процес відновлення та дешифрування цих даних з метою отримання доступу до важливої інформації, яка може бути використана у розслідуванні злочинів або аналізі кібератак. Фахівці використовують спеціалізовані інструменти та програми, такі як цифрові форензичні платформи, для аналізу цих файлів. Ці інструменти дозволяють виявляти, видобувати та дешифрувати зашифровані дані.

HackBrowserData - це інструмент командного рядка для розшифрування та експорту даних браузера (паролів, історії, файлів cookie, закладок, кредитних карток, записів завантажень, localStorage і розширень) з браузера. Він підтримує найпопулярніші браузери і працює на Windows, macOS і Linux.

Під час дослідження основних інструментів комп'ютерної форензики стало очевидним, що ця галузь науки та практики є невід'ємною складовою в сучасному світі інформаційної безпеки. За допомогою спеціалізованих програмних засобів та інструментів, фахівці комп'ютерної форензики можуть здійснювати ретельний аналіз цифрових доказів, виявляти злочини та розкривати кіберзлочинців.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		28

РОЗДІЛ 3 ПОСЛІДОВНЕ ДОСЛІДЖЕННЯ ОБРАЗУ ОС WINDOWS.

FTK IMAGER. Дозволяє захоплювати та аналізувати образи дисків, вилучати файли, створювати звіти та перевіряти цілісність дисків. Все це робить FTK Imager потужним інструментом для проведення електронного розслідування.

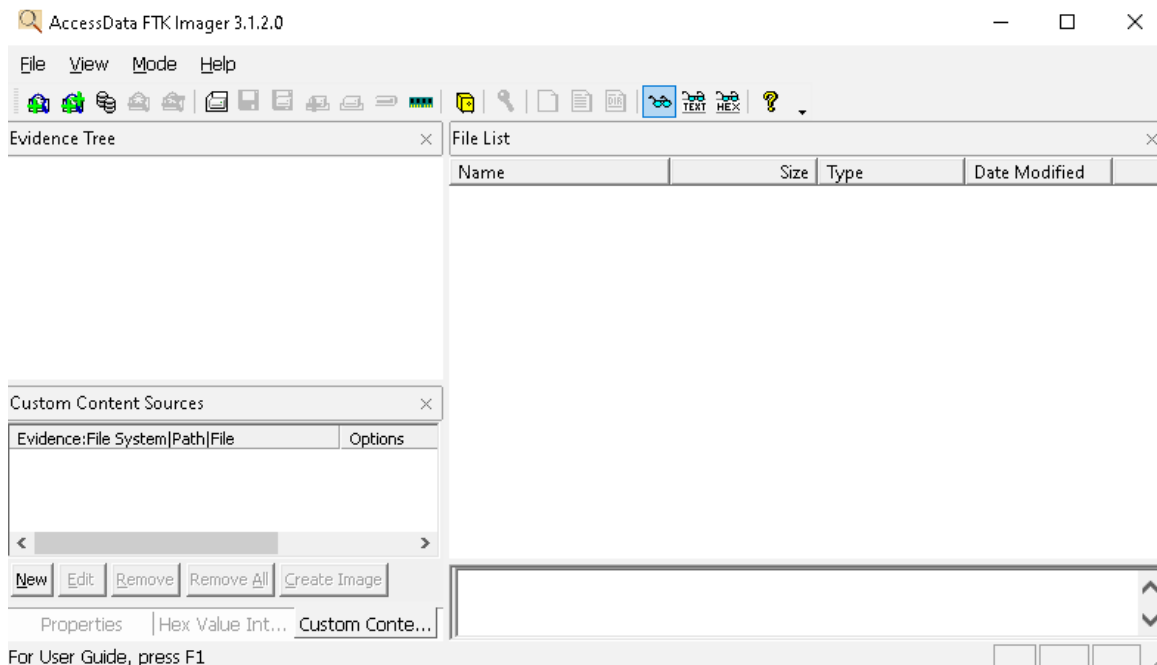


Рисунок 2 – Загальний вигляд ПЗ Autospy.

3.1. Створення образу досліджуваної ОС.

В FTK imager потрібно

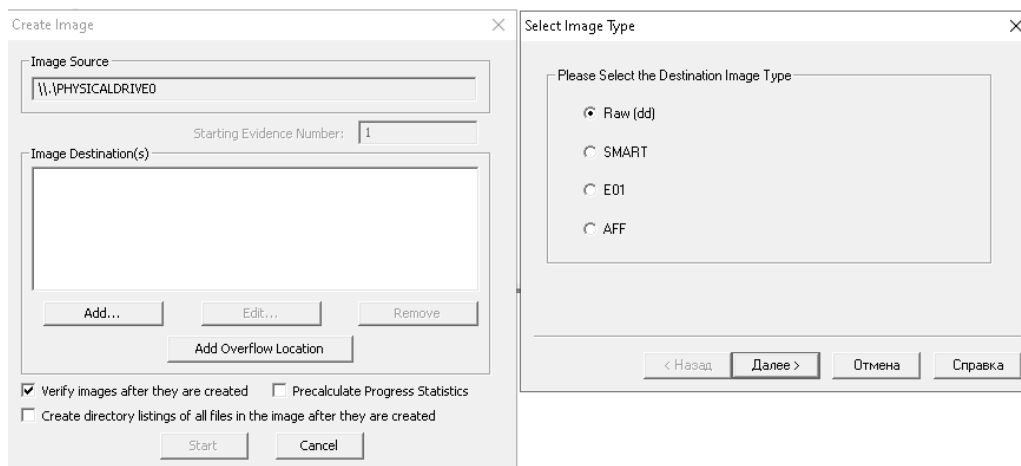


Рисунок 3 – Створення образу та вибір формату.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росініський Ю.М				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Evidence Item Information

Case Number: #4654

Evidence Number: #1

Unique Description: ISO CD

Examiner: OPANASIUK

Notes:

< Назад Далее > Cancel Help

Рисунок 4 – Створення образу та вибір формату

Select Image Destination

Image Destination Folder
B:\ Browse

Image Filename (Excluding Extension)
ISODUMB

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption ☒

< Назад Finish Cancel Help

AD Encryption Credentials

Enter Credentials To Encrypt

☒ Password: *****
Re-enter: ***** ☐ Show password

☐ Certificate (.pfx, .p12, .pem)
Browse

OK Cancel

Рисунок 5 – Вибір диска на який хочемо записати копію та запис паролю на шифрування доказу.

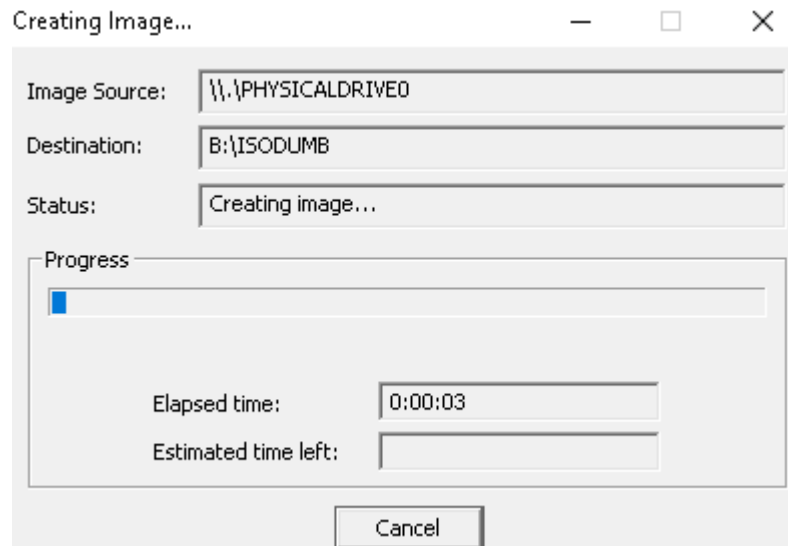


Рисунок 6 – створення образу

3.2. Створення дампу ОЗП.

Основна функція FTK Imager полягає в створенні дампів оперативної пам'яті. Вона дозволяє фіксувати стан пам'яті в певний момент часу, зберігаючи її у вигляді файлу образу. Цей образ пам'яті може бути подальше проаналізований за допомогою спеціалізованих інструментів.

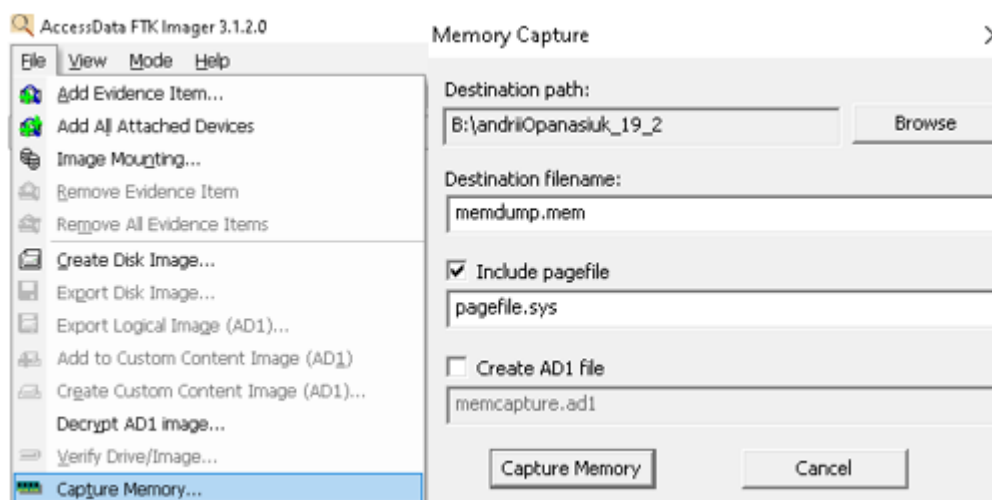


Рисунок 7 – Вибір диску на який хочемо записати копію даних ОЗП.

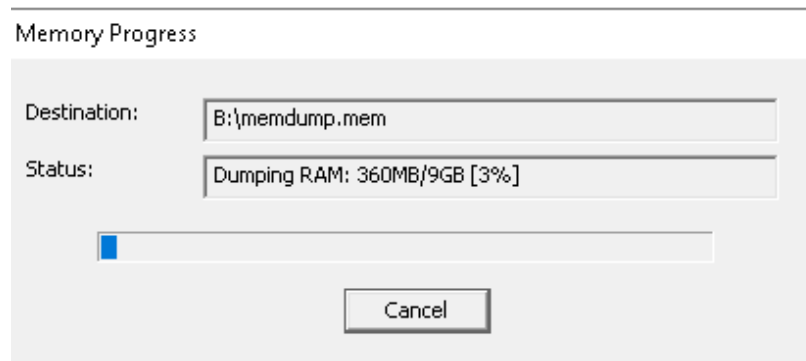


Рисунок 8 – процес створення дампу

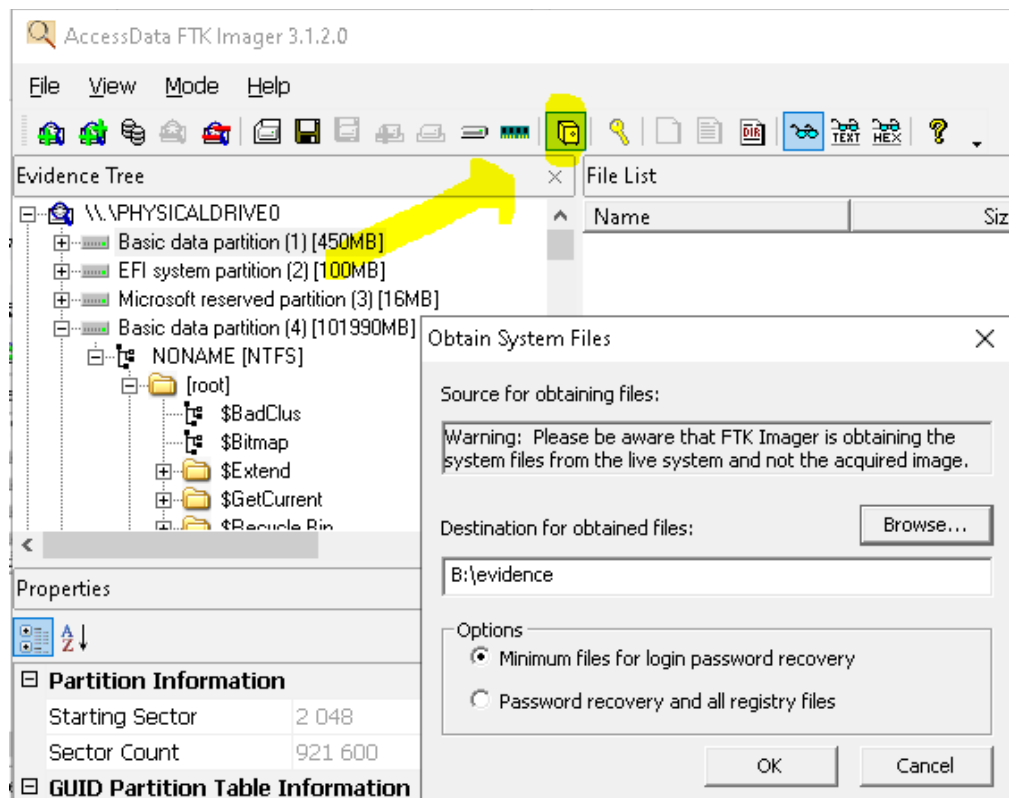


Рисунок 9 – вилучення захищених файлів реєстру та профілів користувача з діючої системи.

На вибір мінімальний та максимальний набір файлів реєстру, ці файли без спеціального ПЗ не вилучити.

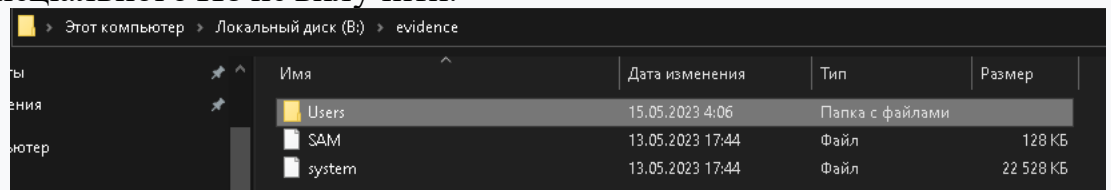


Рисунок 10 – Експорт доказів зокрема файл SAM.

3.3. Витягнення паролів користувачів.

Програма mimikatz дає змогу витягти з пам'яті Windows паролі у вигляді простого тексту, хешів паролів.

Спробуємо витягти хеші паролів усіх залогінених користувачів із пам'яті Windows.

Запустим Mimikatz.exe з правами адміністратора.

```
mimikatz 2.2.0x64 (oe.eo)

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##    > https://blog.gentilkiwi.com/mimikatz
'## v ##'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/
```

Рисунок 11 – Загальний вигляд mimikatz

```
mimikatz # privilege::debug
Privilege '20' OK
```

Рисунок 12 –Ця команда надасть поточному обліковому запису права налагодження процесів (SeDebugPrivilege).

Sekurlsa :: logonPasswords full - ця команда надасть досить великий список. Знайдемо у ньому облікові записи користувачів.

```
mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 81074527 (00000000:04d5195f)
Session           : Interactive from 2
User Name         : hacker
Domain           : DESKTOP-PN5D45V
Logon Server      : DESKTOP-PN5D45V
Logon Time        : 27.06.2023 15:48:57
SID               : S-1-5-21-4223914832-721962193-3762142589-1002

msv :
[00000003] Primary
* Username : hacker
* Domain   : DESKTOP-PN5D45V
* NTLM     : 5e7599f673df11d5c5c4d950f5bf0157
* SHA1     : e8fbe5fa573627767dd153035dd045ab672902c6
tspkg :
wdigest :
* Username : hacker
* Domain   : DESKTOP-PN5D45V
* Password : (null)
kerberos :
* Username : hacker
* Domain   : DESKTOP-PN5D45V
* Password : (null)
ssp :
credman :
cloudap :
```

```

Authentication Id : 0 ; 80924453 (00000000:04d2cf25)
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 27.06.2023 15:48:47
SID               : S-1-5-90-0-2

    msv :
    tspkg :
    wdigest :
        * Username : DESKTOP-PN5D45V$
        * Domain   : WORKGROUP
        * Password : (null)
    kerberos :
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 80920977 (00000000:04d2c191)
Session           : Interactive from 2
User Name         : UMFD-2
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 27.06.2023 15:48:47
SID               : S-1-5-96-0-2

    msv :
    tspkg :
    wdigest :
        * Username : DESKTOP-PN5D45V$
        * Domain   : WORKGROUP
        * Password : (null)
    kerberos :
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 256926 (00000000:0003eb9e)
Session           : Interactive from 1
User Name         : Я
Domain            : DESKTOP-PN5D45V
Logon Server      : DESKTOP-PN5D45V

```

Рисунок 12,13 – лістинг списку користувачів

Знайдем у лістингу потрібного нам користувача та прочитаємо його данні.
 Нам потрібні NTLM хеш для знайдення паролю користувача.

```

Authentication Id : 0 ; 81074527 (00000000:04d5195f)
Session           : Interactive from 2
User Name         : hacker
Domain            : DESKTOP-PN5D45V
Logon Server      : DESKTOP-PN5D45V
Logon Time        : 27.06.2023 15:48:57
SID               : S-1-5-21-4223914832-721962193-3762142589-1002

msv :
[00000003] Primary
* Username : hacker
* Domain   : DESKTOP-PN5D45V
* NTLM     : 5e7599f673df11d5c5c4d950f5bf0157
* SHA1     : e8fbe5fa573627767dd153035dd045ab672902c6

tspkg :
wdigest :
* Username : hacker
* Domain   : DESKTOP-PN5D45V
* Password : (null)

kerberos :
* Username : hacker
* Domain   : DESKTOP-PN5D45V
* Password : (null)

```

Рисунок 12 – дані користувача hacker

NTLM hash користувача hacker - 5e7599f673df11d5c5c4d950f5bf0157

Тепер потрібно розшифрувати хеш я буду використовувати сервіс <https://crackstation.net/>. CrackStation використовує величезні заздалегідь обчислені таблиці пошуку для злому хешів паролів. У цих таблицях зберігається відповідність між хешем пароля і правильним паролем для цього хешу. Значення хешів індексуються, щоб можна було швидко знайти потрібний хеш у базі даних. Якщо хеш присутній в базі даних, пароль можна відновити за частки секунди.

The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with 'Password Hashing Security' and 'Defuse Security' menus. Below that, the title 'Free Password Hash Cracker' is displayed. A text input area is labeled 'Enter up to 20 non-salted hashes, one per line:'. The NTLM hash '5e7599f673df11d5c5c4d950f5bf0157' is entered and highlighted in yellow. To the right of the input field is a CAPTCHA challenge with the text 'Я не робот' and a 'Crack Hashes' button. Below the input field, a list of supported hash types is shown, including LM, NTLM, md2, md4, md5, and others.

Рисунок 13 – загальний вигляд сайту з розшифрування NTLM хешу

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росініський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Hash	Type	Result
5e7599f673df11d5c5c4d950f5bf0157	NTLM	hacker

Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

Рисунок 13 – Лістинг розшифрування NTLM хешу.

Отже, ми отримали інформацію про всіх користувачів. Знайшли потрібного нам для аналізу та розшифрували пароль “hacker”. Як ви бачите, завдяки mimikatz ми отримали NTLM хеші всіх активних користувачів! Усе це завдяки тому, що на цьому комп'ютері дозволено використовувати прапор SeDebugPrivilege для потрібного процесу.

За допомогою mimikatz ви можете витягти хеші паролів локальних користувачів Windows з SAM, який ми отримали раніше за допомогою FTK image (SAM-рисунок 10).

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\СИСТЕМА

688      {0;000003e7} 0 D 59877          NT AUTHORITY\СИСТЕМА    S
-> Impersonated !
* Process Token : {0;0003eb9e} 1 D 82323213    DESKTOP-PN5D45V\A
* Thread Token  : {0;000003e7} 0 D 86552288    NT AUTHORITY\СИСТ

mimikatz # lsadump::sam B:\evidence\SAM
Domain : DESKTOP-PN5D45V
SysKey : 7edd940263d28c080aabd0f3414136c2
Local SID : S-1-5-21-4223914832-721962193-3762142589

SAMKey : f99e0becf5ca879565acb84825b42587

RID : 000001f4 (500)
User : Администратор
Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

RID : 000001f5 (501)
User : Гость

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 7d4704bfc2d20e3bf22a17185b6a0988

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : b19c248f6298de15a2c8903ecabace76

* Primary:Kerberos-Newer-Keys *
Default Salt : DESKTOP-PN5D45VWDAGUtilityAccount
Default Iterations : 4096
Credentials
aes256_hmac (4096) : a55372ea2094e0f7be2a90fa78f3a93c
```

Рисунок 13 – Лістинг розшифрування користувачів та NTLM хешу з дампу файлу SAM.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		36

3.4. Витягнення даних з дампу ОЗП.

Volatility - це фреймворк для аналізу пам'яті з відкритим вихідним кодом для реагування на інциденти та аналізу шкідливого програмного забезпечення. Це дуже потужний інструмент, і ми можемо виконати безліч взаємодій з файлами дампа пам'яті.

Потрібно встановити фреймворк, бібліотеку команд та python. Запускаємо ПЗ через Powershell та обираємо шлях дампу ОЗП – в кінці обираємо, що саме аналізуємо.

```
PS B:\volatility3-2.4.1\volatility3-2.4.1> Python.exe .\vol.py -f B:\hacker\memdumpHacker.mem ВАША КОМАНДА
```

Рисунок 14 – Приклад запуску та обрання дампу.

Список команд для витягнення даних з дампу ОЗП:

windows.bigpools	Список великих пулів сторінок.
windows.callbacks	Перелічує зворотні виклики ядра та підпрограми сповіщень.
windows.cmdline	Перелік аргументів командного рядка процесу.
windows.devicetree	Дерево лістингу на основі драйверів та підключених пристроїв
windows.dlllist	Перелічує завантажені модулі у певному образі пам'яті Windows.
windows.driverirp	Список IRP для драйверів у певному образі пам'яті windows.
windows.drivermodule	Визначає, чи були завантажені драйвери приховані руткітом
windows.driverscan	Сканує наявність драйверів у певному образі пам'яті Windows.
windows.dumpfiles	Збирає дампи вмісту кешованих файлів зі зразків пам'яті
windows.envars	Відображає змінні оточення процесу
windows.filescan	Сканує наявність файлових об'єктів у певному образі пам'яті
windows.getservicesids	Виводить список ідентифікаторів токенів процесів.
windows.getsids	Виводить ідентифікатори SID, що належать кожному процесу
windows.handles	Виводить список відкритих дескрипторів процесів.
windows.info	Показує інформацію про ОС та ядро аналізованого зразка пам'яті.
windows.joblinks	Виводить інформацію про посилання на завдання процесу
windows.malfind	Виводить діапазони пам'яті процесу, які містить ін'єкційний код.
windows.mbrscan	Сканує та аналізує потенційні головні завантажувальні записи
windows.memmap	Виводить на друк мапу пам'яті
windows.modscan	Сканує модулі, присутні у певному образі пам'яті Windows.
windows.modules	Виводить список завантажених модулів ядра.
windows.poolscanner	Типовий плагін для сканування пулу.
windows.privileges	Перелічує привілеї токенів процесів
windows.pslist	Перелічує процеси, присутні у певному образі пам'яті Windows.
windows.psscan	Сканує процеси, присутні у певному образі пам'яті windows.

windows.pstree Плагін для виведення процесів у вигляді дерева на основі ідентифікатора їхніх батьківських процесів.

windows.registry.certificates Виводить список сертифікатів у сховищі

windows.registry.hivelist Перелічує вулики реєстру, наявні у певному образі пам'яті.

windows.registry.hivescan Сканує розділи реєстру, присутні у певному образі пам'яті

windows.registry.printkey Виводить список ключів реєстру під розділом.

windows.sessions виводить список процесів з інформацією про сеанси.

windows.ssdtd Виводить таблицю системних викликів.

windows.statistics Статистика

windows.strings виведення команди strings, і показує якому процесу належить рядок.

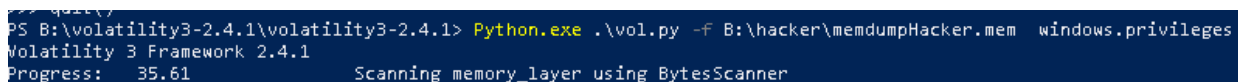
windows.symlinkscan Сканує на наявність посилань у певному образі пам'яті windows.

windows.vadinfo.VadInfo Перелічує діапазони пам'яті процесу.

windows.vadwalk.VadWalk Прогулянка деревом VAD.

windows.virtmap.VirtMap Перелічує віртуальні відмаповані секції.

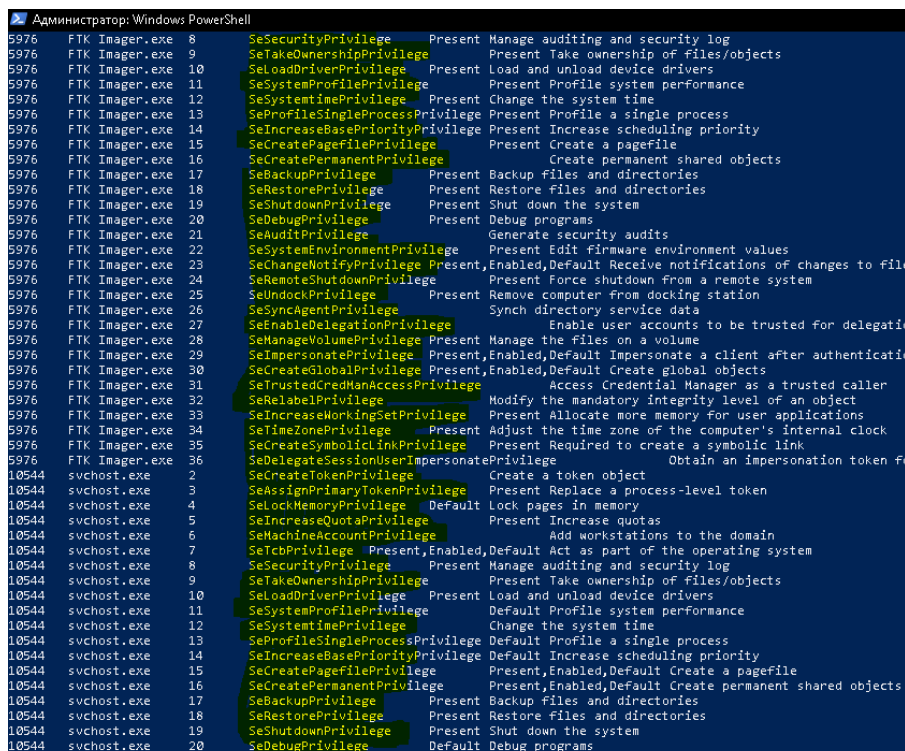
Наведу декілька прикладів витягнення даних з копії ОЗП:



```

PS B:\volatility3-2.4.1\volatility3-2.4.1> Python.exe .\vol.py -f B:\hacker\memdumpHacker.mem windows.privileges
Volatility 3 Framework 2.4.1
Progress: 35.61      Scanning memory_layer using BytesScanner
  
```

Рисунок 15 – Приклад процесу виведення з дампу пам'яті привілеїв процесів Windows.



```

Адміністратор: Windows PowerShell

5976 FTK Imager.exe 8 SeSecurityPrivilege Present Manage auditing and security log
5976 FTK Imager.exe 9 SeTakeOwnershipPrivilege Present Take ownership of files/objects
5976 FTK Imager.exe 10 SeLoadDriverPrivilege Present Load and unload device drivers
5976 FTK Imager.exe 11 SeSystemProfilePrivilege Present Profile system performance
5976 FTK Imager.exe 12 SeSystemTimePrivilege Present Change the system time
5976 FTK Imager.exe 13 SeProfileSingleProcessPrivilege Present Profile a single process
5976 FTK Imager.exe 14 SeIncreaseBasePriorityPrivilege Present Increase scheduling priority
5976 FTK Imager.exe 15 SeCreatePagefilePrivilege Present Create a pagefile
5976 FTK Imager.exe 16 SeCreatePermanentPrivilege Present Create permanent shared objects
5976 FTK Imager.exe 17 SeBackupPrivilege Present Backup files and directories
5976 FTK Imager.exe 18 SeRestorePrivilege Present Restore files and directories
5976 FTK Imager.exe 19 SeShutdownPrivilege Present Shut down the system
5976 FTK Imager.exe 20 SeDebugPrivilege Present Debug programs
5976 FTK Imager.exe 21 SeAuditPrivilege Present Generate security audits
5976 FTK Imager.exe 22 SeSystemEnvironmentPrivilege Present Edit firmware environment values
5976 FTK Imager.exe 23 SeChangeNotifyPrivilege Present,Enabled,Default Receive notifications of changes to file
5976 FTK Imager.exe 24 SeRemoteShutdownPrivilege Present Force shutdown from a remote system
5976 FTK Imager.exe 25 SeUndockPrivilege Present Remove computer from docking station
5976 FTK Imager.exe 26 SeSyncAgentPrivilege Present Synch directory service data
5976 FTK Imager.exe 27 SeEnableDelegationPrivilege Present Enable user accounts to be trusted for delegatio
5976 FTK Imager.exe 28 SeManageVolumePrivilege Present Manage the files on a volume
5976 FTK Imager.exe 29 SeImpersonatePrivilege Present,Enabled,Default Impersonate a client after authenticatio
5976 FTK Imager.exe 30 SeCreateGlobalPrivilege Present,Enabled,Default Create global objects
5976 FTK Imager.exe 31 SeTrustedCredManAccessPrivilege Present Access Credential Manager as a trusted caller
5976 FTK Imager.exe 32 SeRelabelPrivilege Present Modify the mandatory integrity level of an object
5976 FTK Imager.exe 33 SeIncreaseWorkingSetPrivilege Present Allocate more memory for user applications
5976 FTK Imager.exe 34 SeTimeZonePrivilege Present Adjust the time zone of the computer's internal clock
5976 FTK Imager.exe 35 SeCreateSymbolicLinkPrivilege Present Required to create a symbolic link
5976 FTK Imager.exe 36 SeDelegateSessionUserImpersonatePrivilege Present Obtain an impersonation token fo
10544 svchost.exe 2 SeCreateTokenPrivilege Present Create a token object
10544 svchost.exe 3 SeAssignPrimaryTokenPrivilege Present Replace a process-level token
10544 svchost.exe 4 SeLockMemoryPrivilege Default Lock pages in memory
10544 svchost.exe 5 SeIncreaseQuotaPrivilege Present Increase quotas
10544 svchost.exe 6 SeMachineAccountPrivilege Present Add workstations to the domain
10544 svchost.exe 7 SeTcbPrivilege Present,Enabled,Default Act as part of the operating system
10544 svchost.exe 8 SeSecurityPrivilege Present Manage auditing and security log
10544 svchost.exe 9 SeTakeOwnershipPrivilege Present Take ownership of files/objects
10544 svchost.exe 10 SeLoadDriverPrivilege Present Load and unload device drivers
10544 svchost.exe 11 SeSystemProfilePrivilege Present Profile system performance
10544 svchost.exe 12 SeSystemTimePrivilege Present Change the system time
10544 svchost.exe 13 SeProfileSingleProcessPrivilege Present Profile a single process
10544 svchost.exe 14 SeIncreaseBasePriorityPrivilege Present Default Increase scheduling priority
10544 svchost.exe 15 SeCreatePagefilePrivilege Present,Enabled,Default Create a pagefile
10544 svchost.exe 16 SeCreatePermanentPrivilege Present,Enabled,Default Create permanent shared objects
10544 svchost.exe 17 SeBackupPrivilege Present Backup files and directories
10544 svchost.exe 18 SeRestorePrivilege Present Restore files and directories
10544 svchost.exe 19 SeShutdownPrivilege Present Shut down the system
10544 svchost.exe 20 SeDebugPrivilege Default Debug programs
  
```

Рисунок 15 – лістинг команди

		Опанасюк А.М			Арк.
		Росієвський Ю.М			38
Змн.	Арк.	№ докум.	Підпис	Дата	

ККІКБ.КР.Б – 125 – 12 – ПЗ

```

PS B:\volatility3-2.4.1\volatility3-2.4.1> Python.exe .\vol.py -f B:\hacker\memdumpHacker.mem windows.sessions
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
Session ID Session Type Process ID Process User Name Create Time
N/A - 4 System - 2023-06-25 07:08:55.000000
N/A - 100 Registry - 2023-06-25 07:08:45.000000
N/A - 368 smss.exe - 2023-06-25 07:08:55.000000
0 - 492 smss.exe - 2023-06-25 07:09:01.000000
0 - 500 csrss.exe /SYSTEM 2023-06-25 07:09:01.000000
0 - 588 wininit.exe /SYSTEM 2023-06-25 07:09:03.000000
0 - 664 services.exe /SYSTEM 2023-06-25 07:09:04.000000
0 - 688 lsass.exe /SYSTEM 2023-06-25 07:09:04.000000
0 - 880 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:04.000000
0 - 908 fontdrvhost.ex Font Driver Host/UMFD-0 2023-06-25 07:09:04.000000
0 - 992 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:04.000000
0 - 392 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:04.000000
0 - 1096 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1208 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 1288 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1308 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1392 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 1420 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1528 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 1556 NVDIplay.Cont WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1656 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 1756 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 1772 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 1828 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 1868 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1904 igfxCUIService WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1928 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1988 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 1996 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:05.000000
0 - 1124 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:05.000000
0 - 2256 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:06.000000
0 - 2280 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:06.000000
0 - 2364 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:06.000000
0 - 2372 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:06.000000
0 - 2380 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:06.000000
0 - 2632 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:07.000000
0 - 2664 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:07.000000
0 - 2752 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:07.000000
0 - 2920 svchost.exe WORKGROUP/DESKTOP-PN5D45V$ 2023-06-25 07:09:07.000000
0 - 2996 svchost.exe NT AUTHORITY/LOCAL SERVICE 2023-06-25 07:09:07.000000

```

Рисунок 16 – лістинг сесій процесів у ОС Windows

Щоб перерахувати процеси системи, скористайтеся командою pslist:

```

PS B:\volatility3-2.4.1\volatility3-2.4.1> Python.exe .\vol.py -f B:\hacker\memdumpHacker.mem windows.psscan
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output
4 0 System 0x960F482b4080 130 - N/A False 2023-06-25 07:08:55.000000 N/A Disabled
2280 664 svchost.exe 0x960F482d8080 12 - 0 False 2023-06-25 07:09:06.000000 N/A Disabled
100 4 Registry 0x960F482e6080 4 - N/A False 2023-06-25 07:08:45.000000 N/A Disabled
500 492 csrss.exe 0x960F48be1140 10 - 0 False 2023-06-25 07:09:01.000000 N/A Disabled
908 588 fontdrvhost.ex 0x960F4b51b140 5 - 0 False 2023-06-25 07:09:04.000000 N/A Disabled
368 4 smss.exe 0x960F4bc53040 2 - N/A False 2023-06-25 07:08:55.000000 N/A Disabled
6948 664 svchost.exe 0x960F4bce3340 6 - 0 False 2023-06-25 07:09:47.000000 N/A Disabled
912 760 fontdrvhost.ex 0x960F4cb5b300 5 - 1 False 2023-06-25 07:09:04.000000 N/A Disabled
492 368 smss.exe 0x960F4cb6d240 0 - 0 False 2023-06-25 07:09:01.000000 2023-06-25 07:09:03.000000 Disabled
992 664 svchost.exe 0x960F4cb75240 12 - 0 False 2023-06-25 07:09:04.000000 N/A Disabled
880 664 svchost.exe 0x960F4d92a240 18 - 0 False 2023-06-25 07:09:04.000000 N/A Disabled
580 368 smss.exe 0x960F4dc25080 0 - 1 False 2023-06-25 07:09:03.000000 2023-06-25 07:09:04.000000 Disabled
588 492 wininit.exe 0x960F4dc2c080 1 - 0 False 2023-06-25 07:09:03.000000 N/A Disabled
600 580 csrss.exe 0x960F4dc31140 13 - 1 False 2023-06-25 07:09:03.000000 N/A Disabled
664 588 services.exe 0x960F4dc97280 8 - 0 False 2023-06-25 07:09:04.000000 N/A Disabled
688 588 lsass.exe 0x960F4dc2240 9 - 0 False 2023-06-25 07:09:04.000000 N/A Disabled
760 580 winlogon.exe 0x960F4dcd0100 7 - 1 False 2023-06-25 07:09:04.000000 N/A Disabled
392 664 svchost.exe 0x960F4dd08080 5 - 0 False 2023-06-25 07:09:04.000000 N/A Disabled
832 760 dwm.exe 0x960F4de891c0 18 - 1 False 2023-06-25 07:09:04.000000 N/A Disabled
1044 880 RuntimeBroker. 0x960F4de8c080 4 - 1 False 2023-06-25 07:09:20.000000 N/A Disabled
6500 1116 msedge.exe 0x960F4df10080 18 - 1 False 2023-06-25 07:21:50.000000 N/A Disabled
1096 664 svchost.exe 0x960F4df26080 7 - 0 False 2023-06-25 07:09:05.000000 N/A Disabled
1116 4800 msedge.exe 0x960F4df95080 75 - 1 False 2023-06-25 07:12:07.000000 N/A Disabled

```

Рисунок 16 – лістинг команди pslist

```

PS B:\volatility3-2.4.1\volatility3-2.4.1> Python.exe .\vol.py -f B:\hacker\memdumpHacker.mem windows.devicetree
Volatility 3 Framework 2.4.1
Progress: 100.00
PDB scanning finished
Offset Type DriverName DeviceName DriverNameOfAttDevice DeviceType
0x960f48273b60 DRV PnpManager N/A N/A N/A
* 0x960f48273b60 DEV PnpManager 00000011 N/A FILE_DEVICE_CONTROLLER
** 0x960f48273b60 ATT PnpManager RdpBus \Driver\rdpbus UNKNOWN
0x960f48274060 DRV pci N/A N/A N/A
* 0x960f48274060 DEV pci NTPNP_PCI0017 N/A FILE_DEVICE_UNKNOWN
** 0x960f48274060 ATT pci NDMP2 \Driver\rt640x64 FILE_DEVICE_PHYSICAL_NETCARD
0x960f48279120 DRV WindowsTrustedRTProxy N/A N/A N/A
0x960f4828edf0 DRV Wdf01000 N/A N/A N/A
* 0x960f4828edf0 DEV Wdf01000 KMDF0 N/A FILE_DEVICE_UNKNOWN
0x960f48291390 DRV RAW N/A N/A N/A
* 0x960f48291390 DEV RAW RawTape N/A FILE_DEVICE_TAPE_FILE_SYSTEM
0x960f482b6d60 DRV intelpep N/A N/A N/A
0x960f482b9940 DRV partmgr N/A N/A N/A
* 0x960f482b9940 DEV partmgr - N/A FILE_DEVICE_DISK
0x960f482cb800 DRV ACPI N/A N/A N/A
* 0x960f482cb800 DEV ACPI - N/A FILE_DEVICE_ACPI
** 0x960f482cb800 ATT ACPI 00000042 \Driver\usbccgp FILE_DEVICE_UNKNOWN
0x960f482cde00 DRV SoftwareDevice N/A N/A N/A
* 0x960f482cde00 DEV SoftwareDevice 0000005c N/A FILE_DEVICE_UNKNOWN
** 0x960f482cde00 ATT SoftwareDevice NDMP10 \Driver\NdisWan FILE_DEVICE_PHYSICAL_NETCARD
0x960f482e8db0 DRV ACPI_HAL N/A N/A N/A
* 0x960f482e8db0 DEV ACPI_HAL 00000012 N/A FILE_DEVICE_BUS_EXTENDER
** 0x960f482e8db0 ATT ACPI_HAL - \Driver\ACPI FILE_DEVICE_ACPI
0x960f482f5db0 DRV WMIxWDM N/A N/A N/A
* 0x960f482f5db0 DEV WMIxWDM WMIDataDevice N/A FILE_DEVICE_UNKNOWN
0x960f482f7e00 DRV DeviceApi N/A N/A N/A
* 0x960f482f7e00 DEV DeviceApi DeviceApi N/A FILE_DEVICE_UNKNOWN
0x960f4830e6d0 DRV pdc N/A N/A N/A
* 0x960f4830e6d0 DEV pdc - N/A FILE_DEVICE_UNKNOWN
0x960f4830ed80 DRV acpiex N/A N/A N/A
* 0x960f4830ed80 DEV acpiex RESOURCE_HUB N/A FILE_DEVICE_UNKNOWN
0x960f48328d30 DRV CNG N/A N/A N/A
* 0x960f48328d30 DEV CNG CNG N/A UNKNOWN
0x960f48330a80 DRV MsSecCore N/A N/A N/A
0x960f48330c90 DRV SgrmAgent N/A N/A N/A
* 0x960f48330c90 DEV SgrmAgent HSSGRMAGENTSYS N/A FILE_DEVICE_UNKNOWN
0x960f48339c90 DRV WindowsTrustedRT N/A N/A N/A
* 0x960f48339c90 DEV WindowsTrustedRT WindowsTrustedRT N/A FILE_DEVICE_UNKNOWN
0x960f4834aa80 DRV Telemetry N/A N/A N/A
0x960f483886d0 DRV vdrvroot N/A N/A N/A
* 0x960f483886d0 DEV vdrvroot - N/A FILE_DEVICE_BUS_EXTENDER
0x960f483efa70 DRV msisadrv N/A N/A N/A
* 0x960f483efa70 DEV msisadrv - N/A FILE_DEVICE_UNKNOWN

```

Рисунок 17 – Дерево лістингу на основі драйверів та підключених пристроїв

```

PS B:\volatility3-2.4.1\volatility3-2.4.1> Python.exe .\vol.py -f B:\hacker\memdumpHacker.mem windows.cmdline
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
PID Process Args
4 System Required memory at 0x20 is not valid (process exited?)
100 Registry Required memory at 0x20 is not valid (process exited?)
368 smss.exe \SystemRoot\System32\smss.exe
492 smss.exe Required memory at 0xcfb6b8020 is not valid (process exited?)
500 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768
Initialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
580 smss.exe Required memory at 0x5810a42020 is not valid (process exited?)
588 wininit.exe wininit.exe
600 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768
Initialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
664 services.exe C:\WINDOWS\system32\services.exe
688 lsass.exe C:\WINDOWS\system32\lsass.exe
760 winlogon.exe winlogon.exe
880 svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
912 fontdrvhost.exe "Fontdrvhost.exe"
908 fontdrvhost.exe "Fontdrvhost.exe"
992 svchost.exe C:\WINDOWS\system32\svchost.exe -k RPCSS -p
992 svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p -s LSM
832 dwm.exe "dwm.exe"
1096 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s hidserv
1208 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
1288 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule
1308 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s ProfSvc
1392 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork -p
1420 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s UserManager
1528 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
1556 NvDisplay.Cont "C:\Program Files\NVIDIA Corporation\Display.NvContainer\NvDisplay.Container.exe" -s
stem.log" -l 3 -d "C:\Program Files\NVIDIA Corporation\Display.NvContainer\plugins\LocalSystem" -r -p 30000
1656 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Eventlog
1756 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s nsi
1772 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s EventSystem
1828 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp

```

Рисунок 18 – Перелік аргументів командного рядка процесу з дампу ОЗП

Volatility надає широкий спектр функцій і можливостей для виявлення і відновлення цифрових слідів з дампів ОЗП, що робить його цінним інструментом для фахівців з комп'ютерної форензики.

3.5 Комплексний аналіз файлової системи за допомогою ПЗ Autopsy

Autopsy є популярним інструментом у сфері комп'ютерної форензики, який надає автоматизований підхід до аналізу цифрових доказів.

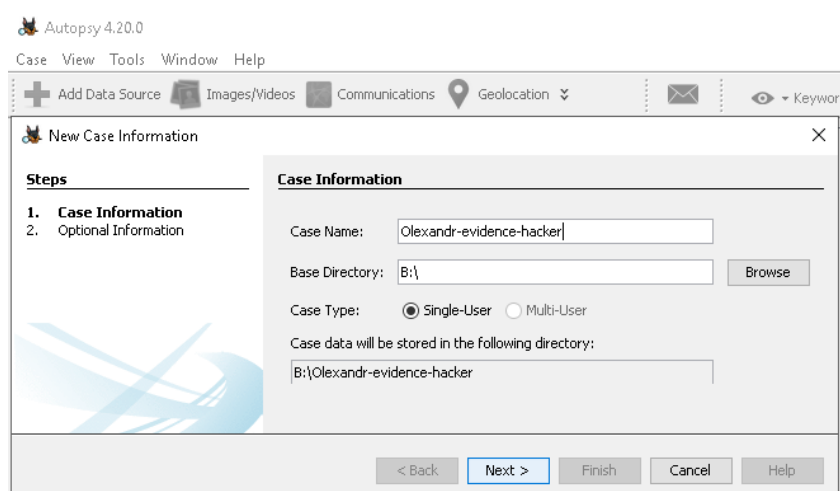


Рисунок 19 – Створення справи

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росінський Ю.М				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Вводимо номер дослідження та дані екзамінатора.

Autopsy 4.20.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Keyword Lists

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: N9192-10-1

Examiner

Name: Andrii

Phone: +40 331 32 32

Email: cyber@forensics.com

Notes:

Organization

Organization analysis is being done for: Politech Forensics Manage Organizations

< Back Next > Finish Cancel Help

Рисунок 20 – Створення справи розслідування.

Далі обираємо об'єкт дослідження. Так як образи ОС займають багато місця, можна використовувати образи віртуальних машин або підключених диск.Я буду проводити аналіз свого диску з підозрілими файлами.

Select Data Source Type

Disk Image or VM File

Local Disk

Рисунок 21 – Вибір джерела даних.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росініський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		42

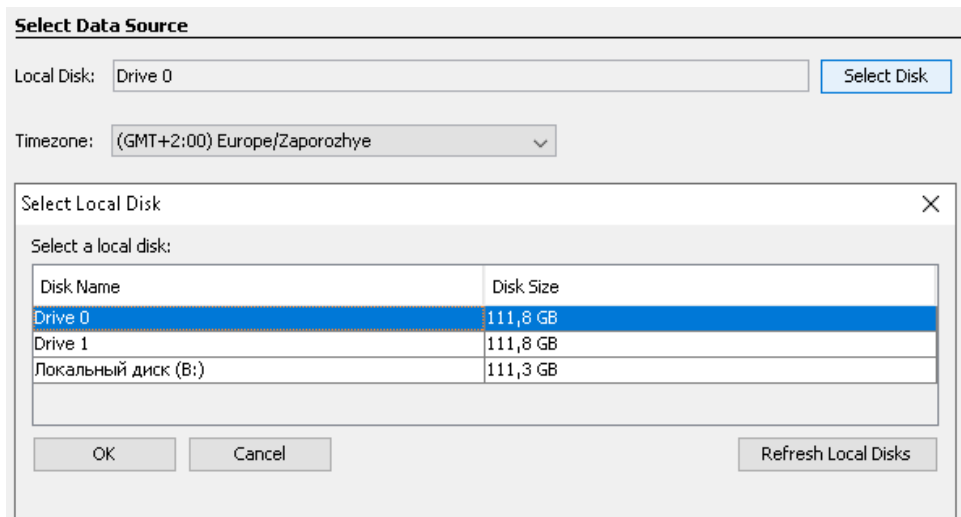


Рисунок 22 – Вибір досліджуваного диску та зони поясу.

Після того як ми додали джерело даних, нам запропонують вибрати модулі. Модулі це інструменти, які виконують аналіз. Кожен із них я описав у 2 розділі. Далі потрібно вибрати їх для аналізу, залишаю за замовченням.

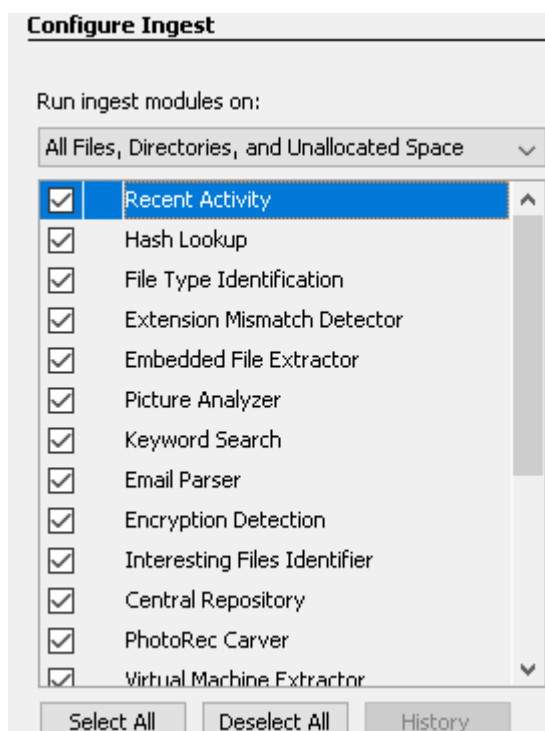


Рисунок 23 – Вибір модулів для дослідження джерела.

Після успішного завершення аналізу нас зустрічає дерево дослідження. Тут відображаються всі джерела, які ми додали в проєкт і за якими було здійснено аналіз. Під час вибору конкретного розділу у вікні, побачимо його вміст, тобто файли і каталоги, а також інформацію що до них.

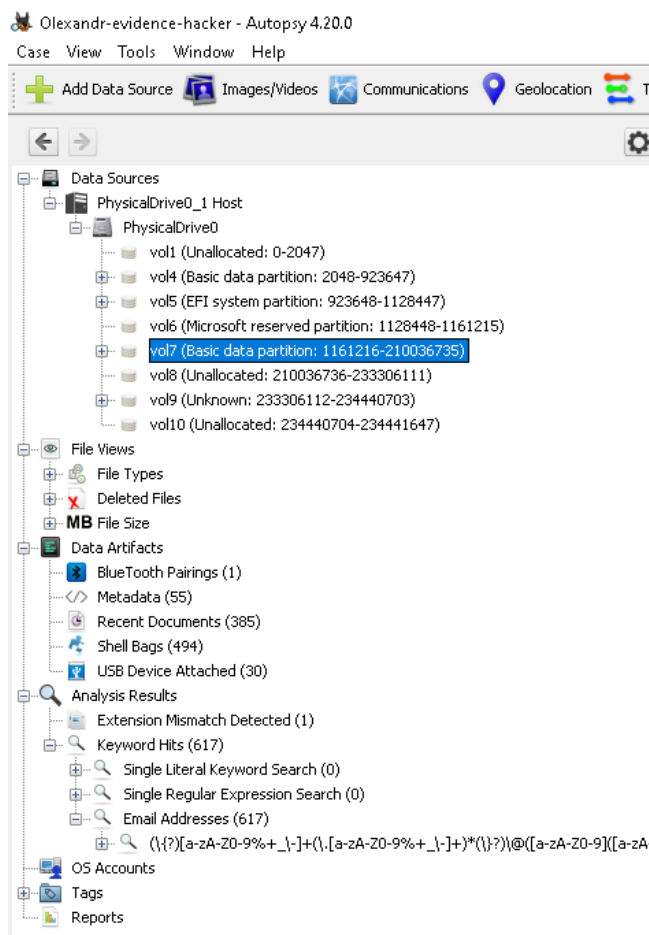


Рисунок 24 – Дерево дослідження

Дерево “File Views”:

File Types - файли сортуються залежно від типу. Є два типи: за розширенням і за MIME. Виділяються зображення, відео, аудіо, архіви, бази даних, документи і виконувані файли.

Deleted Files - файли, які були виявлені як видалені.

MB File Size - файли сортуються залежно від розміру.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росінський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Data Artifacts - тут зібрані знайдені сліди активності користувачів. Зокрема дані операційної системи, веб-активність у вигляді закладок, кукісів, історії пошуку і відвідування сайтів, ну і так далі. Також сюди буде додано знайдені акаунти та адреси електронних пошт, ну і листи, якщо такі будуть знайдені.

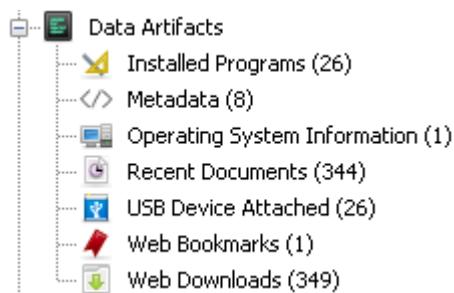


Рисунок 25 – дерево Data artifacts

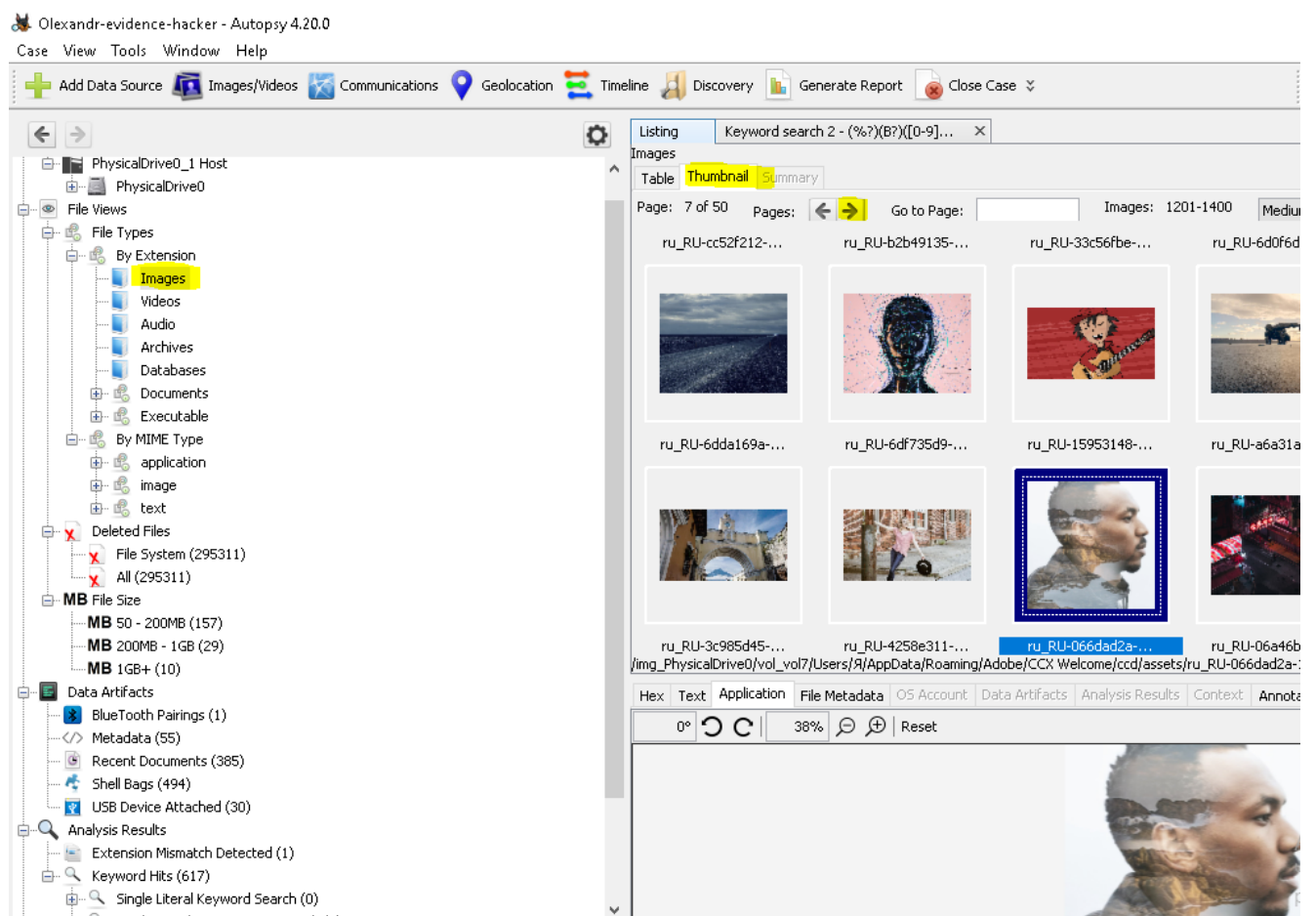


Рисунок 26 – Знайдені фотографії с ОС Windows.

Метаданні зображення з пункту “File Metadata”:

Name:	/img_PhysicalDrive0/vol_vol7/Users/Я/AppData/Roaming/Adobe/CCX Welcome/ccd/assets/ru_RU-066dad2a-1a9a-45e4-bdb5-66468337f523.jpeg
Type:	File System
MIME Type:	image/jpeg
Size:	125987
File Name	Allocated
Allocation:	
Metadata Allocation:	Allocated
Modified:	2023-06-09 18:21:46 GMT+02:00
Accessed:	2023-06-09 18:21:46 GMT+02:00
Created:	2023-06-09 18:21:46 GMT+02:00
Changed:	2023-06-09 18:21:46 GMT+02:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup	UNKNOWN
Results:	
Internal ID:	134843

Так само можна аналізувати й інші розділи. Програма також може витягнути видалені зображення, файли, тощо, до того моменту поки ці дані не будуть перезаписані новою інформацією.

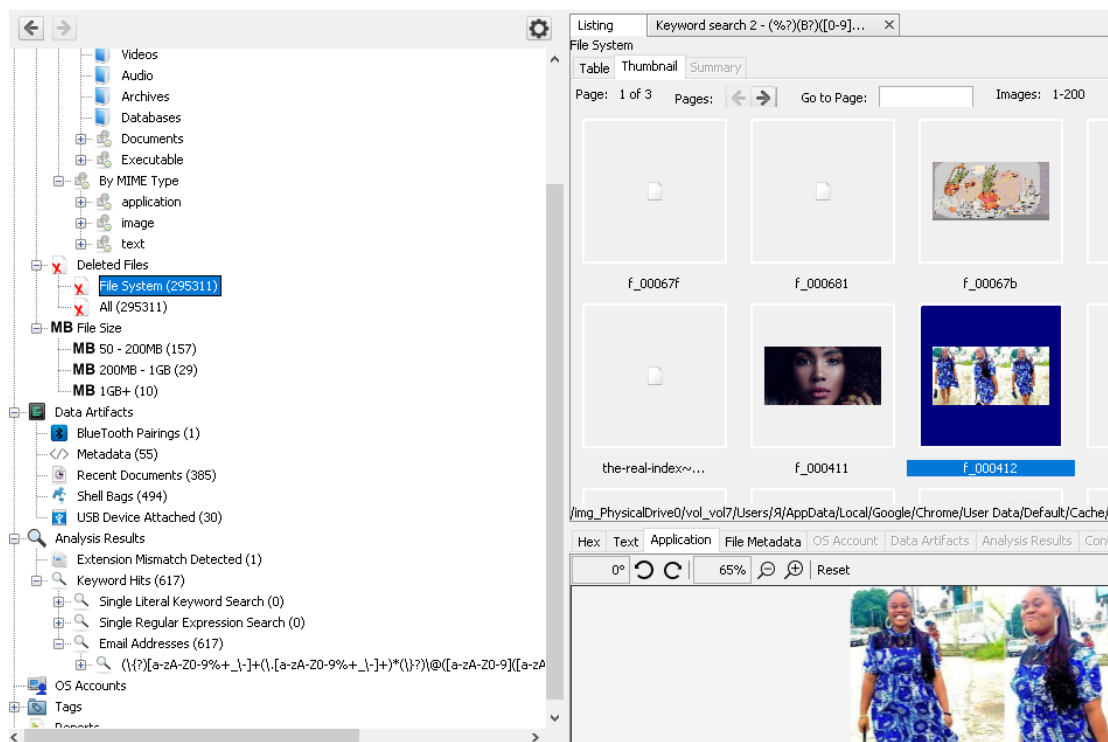


Рисунок 27 – Знайдені видалені фото з ОС Windows.

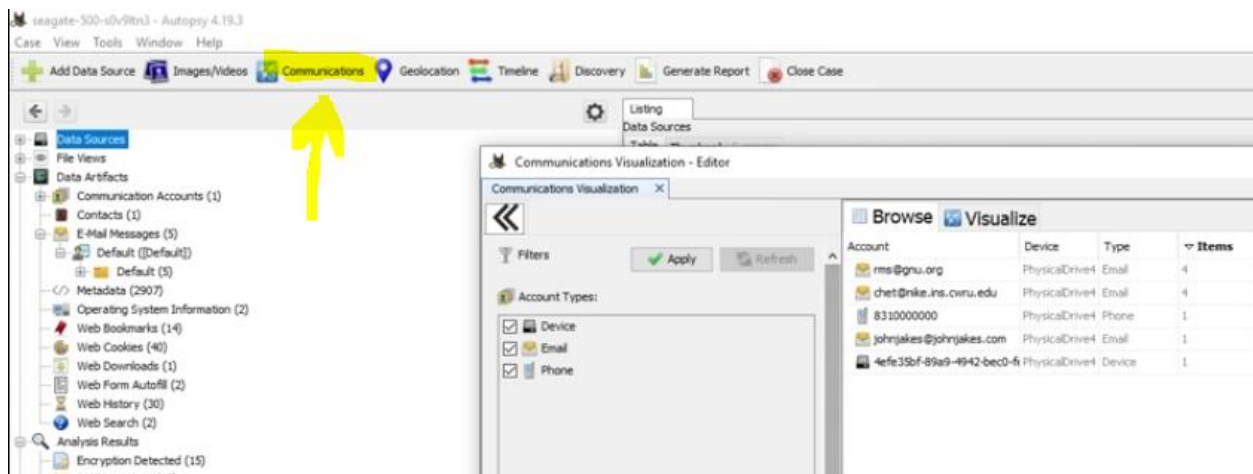


Рисунок 28 – аналіз комунікацій(номери телефони, пошта)

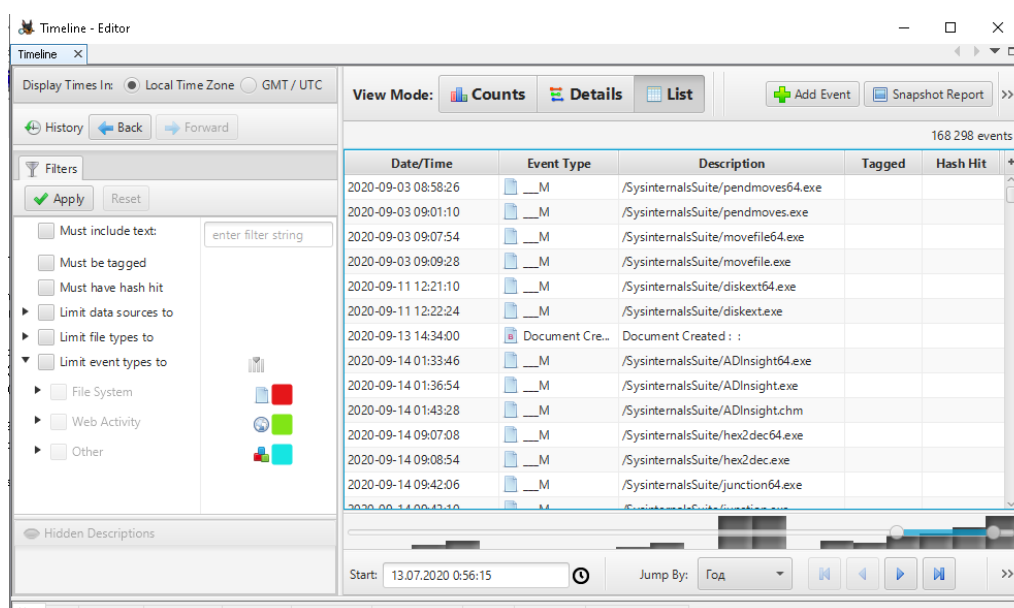


Рисунок 29 – Скриншот дат подій у ОС WINDOWS.

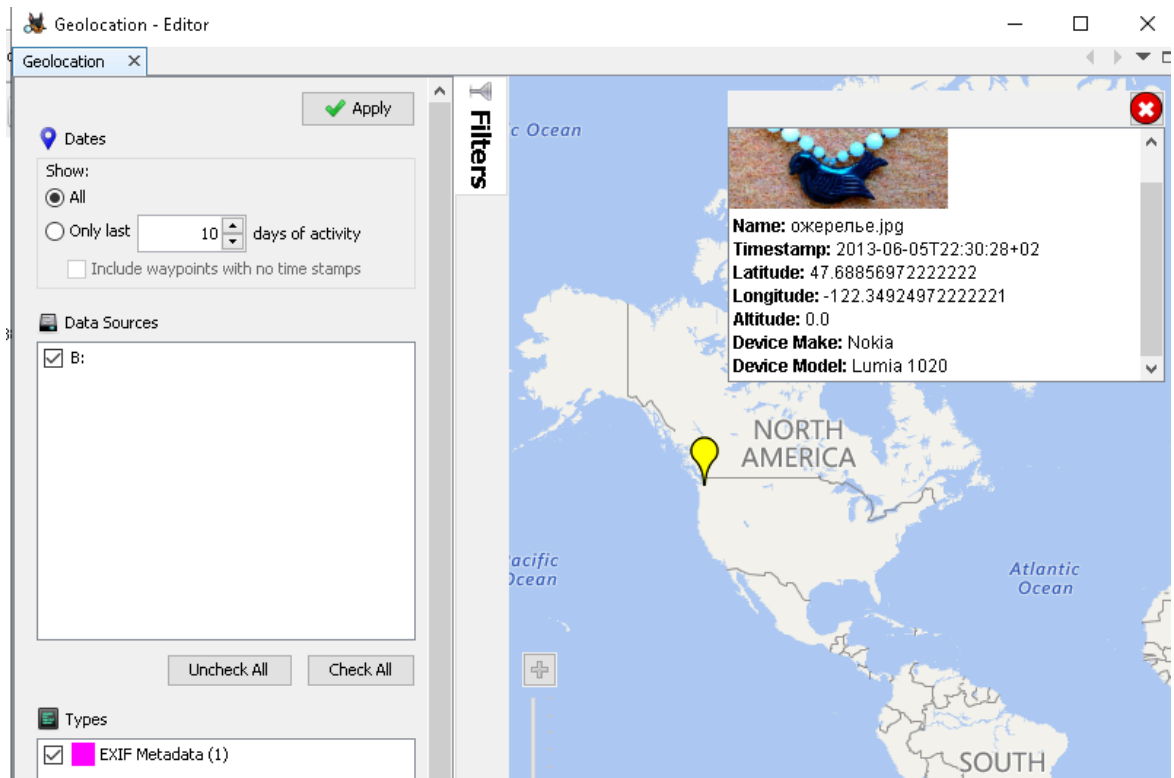


Рисунок 30 – геолокація та дані в момент створення файлу.

Analysis Results – саме тут зібрані результати роботи деяких модулів, на які, Autopsy вважає, що нам потрібно звернути увагу.

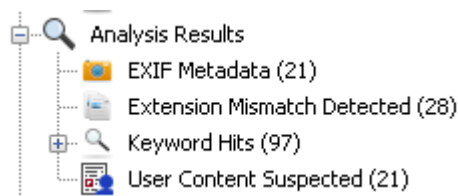


Рисунок 31 – дерево analysis results.

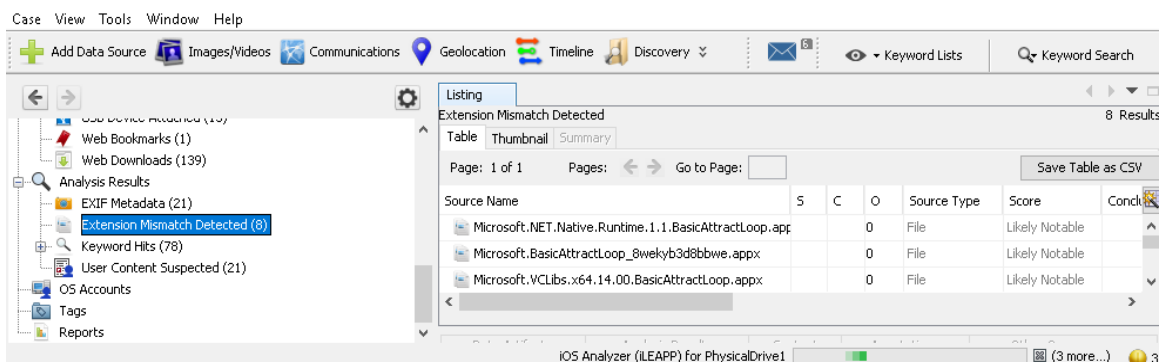


Рисунок 32 – файли у яких розширення не співпадає з типом файла.

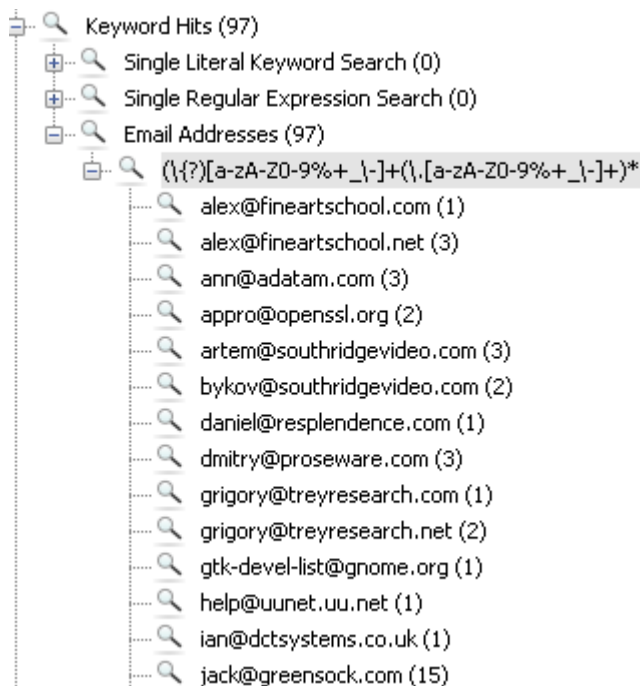


Рисунок 33 – адреса електронних пошт, які знайшла програма.

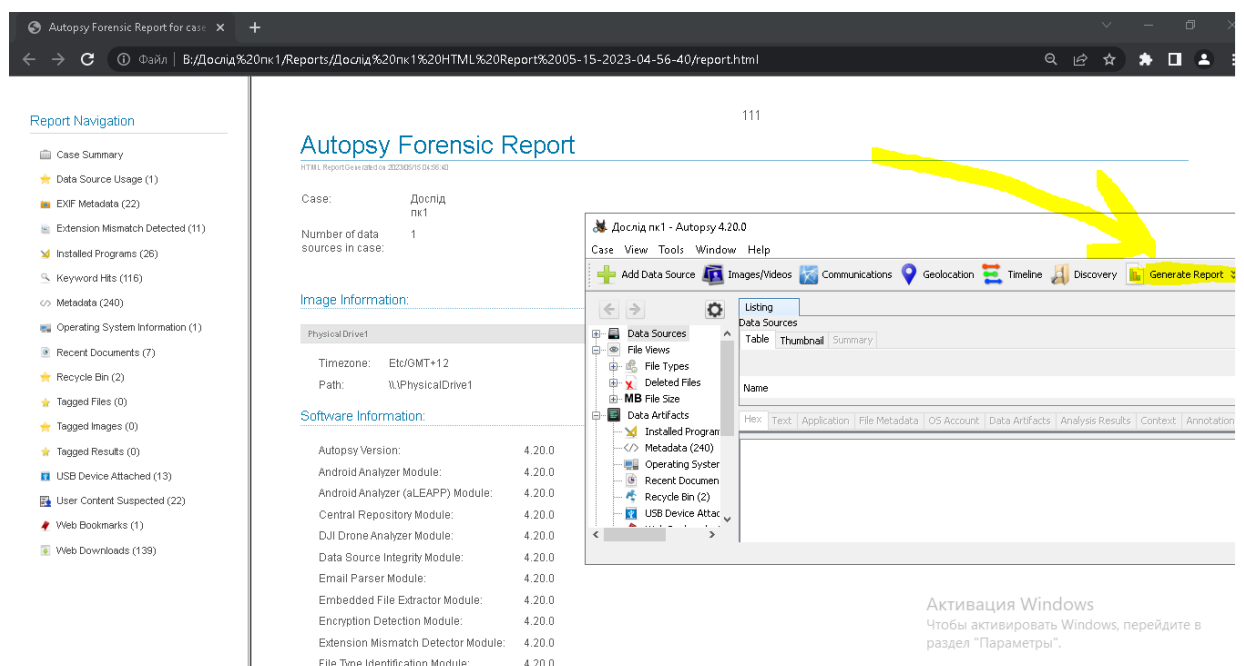


Рисунок 34 - Створення звіту з дослідження об'єкта

AutoSpry є потужним набором інструментів для цифрового розслідування, який надає широкий спектр функцій і можливостей для аналізу цифрових слідів на комп'ютерах і мобільних пристроях.

Один з головних плюсів AutoPsy - це його відкритий джерела коду, що дозволяє експертам з цифрового розслідування адаптувати та розширювати функціональні можливості згідно зі своїми потребами. Це дає можливість гнучкого вико-

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росініський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		49

ристання інструментів для різноманітних завдань, включаючи виявлення зловмисного програмного забезпечення, аналіз файлових систем, відновлення видалених файлів та багато іншого.

3.6 Витягнення даних браузера

HackBrowserData - це інструмент командного рядка для розшифрування та експорту даних браузера (паролів, історії, файлів cookie, закладок, кредитних карток, записів завантажень, localStorage і розширень) з браузера у зручні Excel таблиці. Він підтримує найпопулярніші браузери і працює на Windows, macOS і Linux.

```
B:\hack-browser-data-windows-64bit>hack-browser-data-windows-64bit.exe -h
NAME:
  hack-browser-data - Export passwords/cookies/history/bookmarks from browser

USAGE:
  [hack-browser-data -b chrome -f json -dir results -cc]
  Export all browsingdata(password/cookie/history/bookmark) from browser
  Github Link: https://github.com/moonD4rk/HackBrowserData

VERSION:
  0.4.3

GLOBAL OPTIONS:
  --verbose, --vv                verbose (default: false)
  --compress, --zip              compress result to zip (default: false)
  --browser value, -b value      available browsers: all|360|brave|chrome|chrome-beta|chromium|cocccoc|edge|firefox|opera|opera-gx|qq|vivaldi|yandex (default: "all")
  --results-dir value, --dir value export dir (default: "results")
  --format value, -f value       file name csv|json (default: "csv")
  --profile-path value, -p value custom profile dir path, get with chrome://version
  --help, -h                     show help (default: false)
  --version, -v                  print the version (default: false)
```

Рисунок 35 – запуск інструмента та перегляд команд.

```
B:\hack-browser-data-windows-64bit>hack-browser-data-windows-64bit.exe --zip
[NOTICE] [browser.go:51,pickChromium] find browser Microsoft Edge success
[NOTICE] [browser.go:53,pickChromium] find browser microsoft_edge_default success
[NOTICE] [browser.go:47,pickChromium] find browser Vivaldi failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser CocCoc failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Yandex failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser 360speed failed, profile folder does not exist
[NOTICE] [browser.go:51,pickChromium] find browser Chrome success
[NOTICE] [browser.go:53,pickChromium] find browser chrome_guest_user success
[NOTICE] [browser.go:53,pickChromium] find browser chrome_user_1 success
[NOTICE] [browser.go:53,pickChromium] find browser chrome_default success
[NOTICE] [browser.go:47,pickChromium] find browser Chrome Beta failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Opera failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser OperaGX failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Brave failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser QQ failed, profile folder does not exist
[NOTICE] [browser.go:47,pickChromium] find browser Chromium failed, profile folder does not exist
[NOTICE] [browser.go:91,pickFirefox] find browser firefox Firefox failed, profile folder does not exist
```

Рисунок 36 – витягнення даних у архів.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росініський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		50

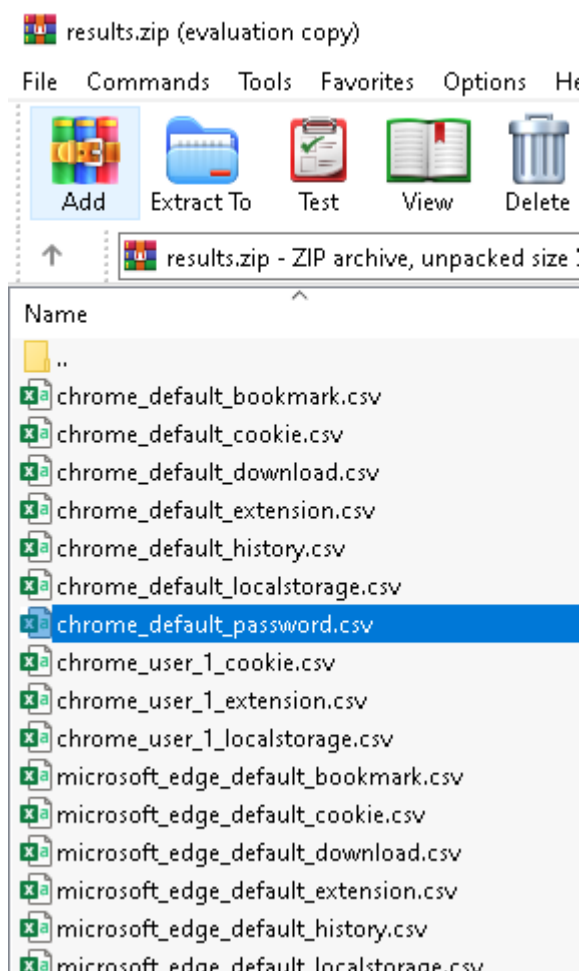


Рисунок 37– результати.

	A	B	C	D	E	F
4	23,Digital Forensic Memory Analysis - Volatility - YouTube,u					
5	22,Forensic Memory Acquisition in Windows - FTK Imager -					
6	21,Starting a New Digital Forensic Investigation Case in Aut					
7	20,КЭ.Практическая работа №1 - Обзор утилиты Autopsy					
8	18,НМП Спецкурс кіберзлочини.pdf,url,http://dspace.onl					
9	17,Восстанавливаем локальные и доменные пароли из h					
10	16,Створення плану (змісту) курсової роботи/реферату -					
11	14,Форензика на НТО по информационной безопасности					

Рисунок 38– Скриншот списка закладок у браузері.

ВИСНОВКИ

Дане дослідження зосереджується на розгляді теоретичних аспектів процесу розслідування кіберінцидентів, загального огляду інструментів комп'ютерної криміналістики та послідовного дослідження образу операційної системи Windows.

Перший розділ присвячений таким аспектам, як забезпечення цілостності доказового матеріалу, збір та аналіз даних, фіксація доказів та звітування, а також постановка технічного завдання.

Другий розділ розглядає загальний огляд інструментів комп'ютерної криміналістики, включаючи інструмент для створення образу операційної системи та дамів ОЗП, перехоплення даних користувача ОС Windows, автоматизоване програмне забезпечення для аналізу даних та витягнення зашифрованих даних з браузерів.

Третій розділ розглядає послідовних кроків дослідження образу операційної системи Windows, включаючи створення копій за допомогою програмного забезпечення FTK Imager, витягнення даних з дампу ОЗП, комплексний аналіз файлової системи з використанням програмного забезпечення Autospy та витягнення даних з браузера за допомогою програмного забезпечення Hack Browser Data.

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієвський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		52

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Autopsy. Data and information recovery - Hacker's Basement. URL: <https://hacker-basement.com/2023/01/09/vosstanovlenie-dannix-autopsy/> (dateofaccess: 22.06.2023).
2. Contributors to Wikimedia projects. Computer forensics - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Computer_forensics (date of access: 22.06.2023).
3. Fox N. How to use volatility for memory forensics and analysis | varonis. *Varonis: We Protect Data*. URL: <https://www.varonis.com/blog/how-to-use-volatility> (date of access: 22.06.2023).
4. GitHub - moond4rk/hackbrowserdata: decrypt passwords/cookies/history/bookmarks from the browser. *GitHub*. URL: <https://github.com/moonD4rk/HackBrowserData> (date of access: 22.06.2023).
5. Volatility-CheatSheet-HackTricks. *HackTricks-HackTricks*. URL: <https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/memory-dump-analysis/volatility-cheatsheet> (dateof access: 22.06.2023).
6. What data forensics? *DigitalGuardian*. URL: <https://www.digitalguardian.com/dskb/data-forensics> (date of access: 22.06.2023).
7. Форе́нзика — ви́кіпедія. *Вікіпедія*. URL: <https://ru.wikipedia.org/wiki/Форе́нзика> (date of access: 22.06.2023).
8. Introduction to Autopsy | An Open-Source Digital Forensics Tool - CYBERVIE. *CYBERVIE*. URL: <https://www.cybervie.com/blog/introduction-to-autopsy-an-open-source-digital-forensics-tool/> (date of access: 22.06.2023).
9. Loshin P. Mimikatz tutorial: How it hacks Windows passwords, credentials | Tech-Target. *Security*. URL: <https://www.techtarget.com/searchsecurity/tutorial/Mimikatz-tutorial-How-it-hacks-Windows-passwords-credentials> (date of access: 22.06.2023).
10. Buckbee M. What is Mimikatz? The Beginner's Guide. *Varonis: We Protect Data*. URL: <https://www.varonis.com/blog/what-is-mimikatz> (date of access: 22.06.2023).

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росі́нський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		53

11. Mimikatz. URL: https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/post-exploitation_mimikatz.htm
(date of access: 28.06.2023).

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієнський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		54

ДОДАТКИ

		Опанасюк А.М			ККІКБ.КР.Б – 125 – 12 – ПЗ	Арк.
		Росієнський Ю.М				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Список команд для витягнення даних з дапу ОЗП:

windows.bigpools	Список великих пулів сторінок.
windows.callbacks	Перелічує зворотні виклики ядра та підпрограми сповіщень.
windows.cmdline	Перелік аргументів командного рядка процесу.
windows.devicetree	Дерево лістингу на основі драйверів та підключених пристроїв
windows.dlllist	Перелічує завантажені модулі у певному образі пам'яті Windows.
windows.driverirp	Список IRP для драйверів у певному образі пам'яті windows.
windows.drivermodule	Визначає, чи були завантажені драйвери приховані руткітом
windows.driverscan	Сканує наявність драйверів у певному образі пам'яті Windows.
windows.dumpfiles	Збирає дампи вмісту кешованих файлів зі зразків пам'яті
windows.envars	Відображає змінні оточення процесу
windows.filescan	Сканує на наявність файлових об'єктів у певному образі пам'яті
windows.getservicesids	Виводить список ідентифікаторів токенів процесів.
windows.getsids	Виводить ідентифікатори SID, що належать кожному процесу
windows.handles	Виводить список відкритих дескрипторів процесів.
windows.info	Показує інформацію про ОС та ядро аналізованого зразка пам'яті.
windows.joblinks	Виводить інформацію про посилання на завдання процесу
windows.malfind	Виводить діапазони пам'яті процесу, які містить ін'єкційний код.
windows.mbrscan	Сканує та аналізує потенційні головні завантажувальні записи
windows.memmap	Виводить на друк мапу пам'яті
windows.modscan	Сканує модулі, присутні у певному образі пам'яті Windows.
windows.modules	Виводить список завантажених модулів ядра.
windows.poolscanner	Типовий плагін для сканування пулу.
windows.privileges	Перелічує привілеї токенів процесів
windows.pslist	Перелічує процеси, присутні у певному образі пам'яті Windows.
windows.psscan	Сканує процеси, присутні у певному образі пам'яті windows.
windows.pstree	Плагін для виведення процесів у вигляді дерева на основі ідентифікатора їхніх батьківських процесів.
windows.registry.certificates	Виводить список сертифікатів у сховищі
windows.registry.hivelist	Перелічує вулики реєстру, наявні у певному образі пам'яті.
windows.registry.hivescan	Сканує розділи реєстру, присутні у певному образі пам'яті
windows.registry.printkey	Виводить список ключів реєстру під розділом.
windows.sessions	виводить список процесів з інформацією про сеанси.
windows.ssdt	Виводить таблицю системних викликів.

windows.statistics Статистика
 windows.strings виведення команди strings, і показує якому процесу належить рядок.
 windows.symlinkscan Сканує наявність посилань у певному образі пам'яті windows.
 windows.vadinfo.VadInfo Перелічує діапазони пам'яті процесу.
 windows.vadwalk.VadWalk Прогулянка деревом VAD.
 windows.virtmap.VirtMap Перелічує віртуальні відмаповані секції

Метаданні зображення з пункту “File Metadata”:

Name:	/img_PhysicalDrive0/vol_vol7/Users/Я/AppData/Roaming/Adobe/CCX Welcome/ccd/assets/ru_RU-066dad2a-1a9a-45e4-bdb5-66468337f523.jpeg
Type:	File System
MIME Type:	image/jpeg
Size:	125987
File Name	Allocated
Allocation:	
Metadata	Allocated
Allocation:	
Modified:	2023-06-09 18:21:46 GMT+02:00
Accessed:	2023-06-09 18:21:46 GMT+02:00
Created:	2023-06-09 18:21:46 GMT+02:00
Changed:	2023-06-09 18:21:46 GMT+02:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup	UNKNOWN
Results:	
Internal ID:	134843